SHIFT④™

API Specifications

Payment Page Services – Form

Version 2.6 | November 2023

Contents

Introduction

The Shift4 Form Hosted Payment Page (HPP) is a ready-to-use payment page fully maintained by Shift4. It enables eCommerce merchants to securely accept payments by hosting sensitive PCI data on Shift4 systems. The form can be embedded in the merchant's checkout flow as an iframe or as a redirect page.

The purpose of this document is to provide an in-depth description of the Shift4 Form HPP specification.

Useful Documents / References

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

- *Source Payment Gateway API* – The Source Payment API specification provides detailed information on processing card-not-present transactions.
- *Source / Shift4 Data Transfer Interface* – In-depth description of the Data Transfer Interface and format specifications of the reports provided by Shift4.

Intended Audience

This document is intended for eCommerce merchants wishing to implement the Form HPP on their websites in order to accept payments.

Certification

All new implementations must undergo 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 may be required if new services or features are to be used.

Publication Identification

Copyright © *Source* Ltd. All rights reserved.

Overview

Introduction

The Form HPP is part of the Shift4 payment page service suite**.** It enables eCommerce merchants to easily implement on their website a ready-to-use secured payment page with a simple API call. This solution ensures that no card data passes through the merchant's website or server, nor is it stored on them. Implementing this solution can significantly reduce the merchant's PCI compliance requirements[1].

By using a redirect request to Shift4 servers, the merchant can start accepting payments immediately.

The Form HPP supports requests for Authorisation, Sale and Token transactions, as well as 3D Secure transactions.

> **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 requires 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 chargebacks disputes raised by cardholders and issuers. Refer to *Appendix D: 3D Secure* for more details.

Alternative payment methods (APM)

The Form Hosted Payment Page offers the option of selecting either payment cards or alternative payment methods (APM) as part of the payment page. Your shopper can select the preferred payment method through a pre-selection page displayed as part of the hosted payment page call.

Quick checkout

---

[1] Merchants implementing the Form HPP solution are required to complete the PCI DSS SAQ "A"

You can offer your shoppers a quick checkout option by saving their card details using the Shift4 Token Engine service. In quick checkout the CVV is a non-mandatory field, creating a quick and smooth checkout experience.

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

User error handling

Your shopper might mistakenly enter inaccurate card details. If the issuer responds with an indication that one or more of the card details is incorrect, the Form Hosted Payment Page can display a suitable message to the shopper requesting a review of the details entered. This feature can improve the conversion rate.

Addresses

Integration address: https://ppskey-int.credorax.com/keypayment/rest/v2/paymentRequest

Production address: https://ppskey.credorax.net/keypayment/rest/v2/paymentRequest

HTTP Specifications

- Protocol: HTTPS
- Method: GET
- Content-Type: application/x-www-form-urlencoded

Security/Authentication

A secured channel should be used for sending redirect requests. The client is authenticated using a SHA256 digital signature which must be sent in the request payload and used for verification before the request is approved.

See *Appendix A: SHA256 Cipher* for further details.

Form HPP Specifications

The Form HPP solution requires basic HTML calls. It supports regular SSL or 3D Secure payments with one single integration.

Form Payment Page Transaction Flow

The Form HPP solution includes two steps:

1. **Redirect** – Redirects the card holder to the Shift4 hosted payment page.
2. **Payment** – PCI data is collected and processed, providing an operation outcome response (Success/Fail).

Figure 1- Transaction Flow Diagram
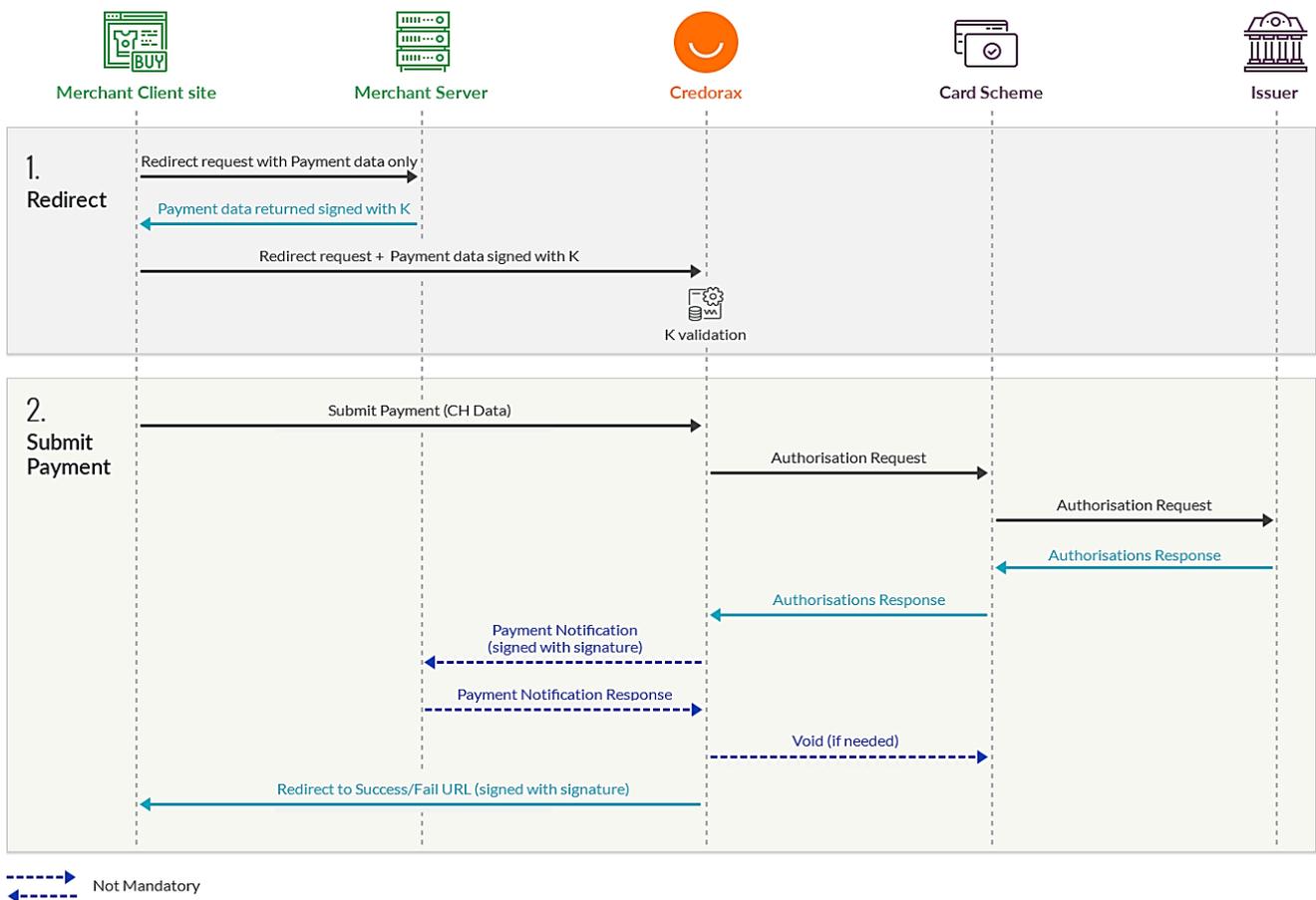
Form Payment Page & 3D Secure Flow

To add a 3D secure layer you can enforce 3D secure authentication via Form HPP. The 3D Secure authentication is fully controlled and managed by Shift4. Relevant 3D Secure tags are added by Shift4 according to the authentication result. Refer to *Appendix D: 3D Secure* for more details.

Payment page & Alternative Payment Methods Flow

The Form Hosted Payment Page offers the option of accepting Alternative Payment Methods (APM) as part of the payment page. If you enrol for the APM service, your shoppers receive a payment selection page where they can choose their preferred payment method from a variety of payment cards and alternative payment methods – depending on the services enabled for your merchant account.

Using the Form HPP with APM entails three steps:

1. **Redirect** – Redirects the shopper to the Shift4 hosted payment method selection page.
2. **Payment selection** – The shopper selects a payment method and based on the selected payment method is redirected to the selected service or asked to fill in the required information.
3. **Payment** – Payment information data is collected and processed, providing an operation outcome response (Success/Fail).

Form HPP API

Step 1 - Redirect Request

This API call enables the customer to create a redirect request for the Shift4 Hosted Payment Page using a GET request. The redirect request must be digitally signed using SHA256 (see *Appendix A: SHA256 Cipher* for more details). The signature must be calculated on the customer server side.

Service name	paymentRequest
Example of a redirect request	https://ppskey-int.credorax.com/keypayment/rest/v2/paymentRequest?K=0000000000&M=10000330&NotificationAddress=&a1=670506320315&a4=80097&a5=EUR&c1=TestUser&c2=&c3=test@credorax.com&c4=&c5=&c7=&c8=&c9=&c10=&shopperID=&i1=&i2=&j1=&j2=&j3=&j4=&O=2&language=en&PurchaseDescription=&ThreeDSecureStatusBehavior=&Skin=1&SuccessURL=https://Success_url_example.com&FailURL=https://Fail_url_example.com&useThreeD=y&Cap=y&other=

Input parameters

Field	Type	Min	Max	m/o/c	Comment
K	[A-Za-Z0-9]	64	64	m	Unique cipher used to authenticate requests. Refer to *Appendix A: SHA256 Cipher* for further details on generating the cipher.
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway Customer ID.

Field	Type	Min	Max	m/o/c	Comment
O	[0-9]	1	2	m	Requested 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** * A token can be used in Form HPP only in a cardholder-initiated transaction, and the cardholder must confirm the payment. To use a token in a merchant-initiated transaction (for example as part of a subscription service), you must implement the Source Payment Gateway API. **If a shopper chooses to save his card details (by selecting the relevant checkbox on the payment page), Form HPP automatically changes the Operation code from 1 or 2 to 23 or 28, respectively.
a1	[a-zA-Z0-9]	8	32	m	Request ID. A unique transaction reference number that must 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.

Field	Type	Min	Max	m/o/c	Comment
a5	[A-Z]	3	3	m	Transaction currency Indicates the currency that should be used in the transaction (every used currency must be pre-configured on the Shift4 platform). Refer to *ISO 4217-alpha-3*. For the supported Shift4 currency list, please refer to *Appendix F: Transaction currencies* in the *Source Gateway Payment API* document.
a8	[a-zA-Z0-9_]	1	16	o	Merchant invoice ID.
NotificationAddress	[a-zA-Z0-9_]	1	32	o	Unique identification of the Payment system server to which the Payment notification should be sent.
shopperID	[a-zA-Z0-9\-]	32	64	o	Shopper ID for using Shift4 token management. The shopperID parameter enables handing over token management to Shift4. The decision whether to save a new card number linked to this shopperID, or to use an existing card, is made by the cardholder as part of the confirmation in the payment page. The cardholder can have multiple cards connected with the same shopperID. The cardholder can decide to delete cards, add new cards or use existing cards. For APMs this value is used to store the shopper's last used payment method. Using this value, we can show the shopper this payment method first when the shopper next makes a purchase.

Field	Type	Min	Max	m/o/c	Comment
c1	[\ a-zA-Z]	5	50	c (recommended – when initiating 3D secure transaction)	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	o	Cardholder's contact phone number. (e.g., 999-999-9999).
c3	[a-zA-Z0-9/.@_]	7	64	o	Email.
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. The 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. If sent, this value will be sent to the issuer and forms part of their AVS checks.
c11	[A_Z]	3	3	c (m for APMs)	Shopper country code

Field	Type	Min	Max	m/o/c	Comment
g1	[a-zA-Z0-9]	1	32	o	The access token for Partner system authorisation stored for this user and payment method.
h3	[0-9]	1	15	o	Sub merchant ID
i1	text	5	64	o	Free text description of the transaction.
i2	text	1	39	o	Relevant only for a merchant who is allowed to use a dynamic descriptor. A Billing Descriptor is the 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 asterisks. 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 a dynamic descriptor. Only the 'city' part (part 3) can be overridden with dynamic content. If the merchant is not configured for a dynamic descriptor, and 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.

Field	Type	Min	Max	m/o/c	Comment
s4	[a-zA-Z0-9]			o	Shipping address line 2
s5	[a-zA-Z0-9]			c (m for PayPal)	Shipping address line 1
s7	[a-zA-Z]			o	Shipping address city
s8	[a-zA-Z]			o	Shipping address state
s9	[A-Z]	3	3	c (m for PayPal)	Shipping address country code
s10	[A-Za-z0-9/s/-]	0	8	o	Shipping address postal code
language	[A-Z]	2	2	o	The language in which the payment page is displayed to the user. Used to display the payment page in the user's native language. Refer to *Appendix E: Supported Languages* for the full list of supported languages. The default value is EN (English).
Skin	[a-zA-Z0-9]	5	8	m	The selected skin of the payment page to be presented. Unique per merchant
SuccessURL	[0-9A-Za-z]	16	512	m	The URL to which the shopper is redirected after a successful transaction (landing page)
FailURL	[0-9A-Za-z]	16	512	m	The URL to which the shopperis redirected after the transaction has failed (landing page)
BackURL	[0-9A-Za-z]	16	512	m	The URL to which the shopperis redirected after clicking the 'Back' option in the payment page (if applicable). By default, this URL is the previous page
order_url	[a-zA-Z0-9]	0	1024	o	The Merchant Site URL related to this payment
cancel_url	[a-zA-Z0-9]	0	1024	c (m for APMs)	The URL to which the user is redirected in case of a cancelled transaction
pending_url	[a-zA-Z0-9]	0	1024	c (m for APMs)	The URL to which the user is redirected in case of a pending transaction

Field	Type	Min	Max	m/o/c	Comment
cap	Text	1	1	o	Boolean field specifying whether to display a captcha object. Possible values: y – yes n – no (default)
other	[0-9A-Za-z/._-]	0	128	o	The "Each other" value, in <key>=value format. This must be the value of the Source Payment Gateway API d2 parameter.
blocked_methods	[a-zA-Z,]	0	256	o	List of all APMs which the merchant does not wish to display. Must be sent in a comma separated list, such as: APM1,APM2
f21	[0-1]	1	1	o	Boolean field specifying whether to bypass the fraud protection service check. 1= Do not send for a fraud check. 0 or N/A= Send for a fraud check. This is the default value. Available only for merchants using the 'Smart Guard Plus' fraud-protection 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 'Smart Guard Plus' fraud-protection service.
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 refer to *Appendix D: 3D Secure*.

Redirect Response

If the K validation is successful, the redirect request is approved, and the cardholder is redirected to the Shift4 secured payment page to enter payment details.

In case of any violation, the redirect request is denied, and the card holder is redirected to a Fail URL.

Step 2 – Payment Response

The result of the processed payment request can be handled in one step or two sub-steps:

1. Notification message (optional): The merchant receives the notification message via an API call and sends a response accordingly. To receive the notification, the merchant must integrate with the HPP payment notification service.

2. Redirect Back to the URL: The cardholder is redirected to the Fail or Success URL you provided in the original redirect request.

Payment Notification (Recommended)

The notification service is recommended to better control the transaction flow through the Form Payment Page; it is applicable to all transactions. 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. You must send a response back to Shift4 upon receiving the notification. If a response is not received, Shift4 instantly cancels the transaction and the shopper is redirected to the 'Fail URL'.

Payment Notification Response

To confirm the notification was received, send '200' in the notification response within 15 seconds of receiving the notification. Any other response, or no response, results in automatic voiding of the transaction.

> **Note:** Automatic voiding consists of four void attempts made in 60 seconds intervals. Note, however, that if all four attempts fail, the transaction might be processed.

Security of the Payment Notification

In the payment notification, Shift4 initiates an HTTP request to the customer's server. The server address is based on the *NotificationAddress* field.

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 please make sure to whitelist our notification server IPs:

Integration address	52.49.236.75
Production address	199.233.202.0/24 199.233.203.0/24

Payment Notification Parameters:

Field	Type	Min	Max	m/o/c	Comment
K	[0-9A-Za-z]	32	64	m	Unique cipher used to authenticate requests. Refer to Appendix A: SHA256 Cipher for further details on generating the cipher.
M	[A-Z0-9_]	3	8	m	Shift4 assigned gateway merchant ID.
T	timestamp	1	32	m	Transaction processing timestamp of type MM/dd/yyyy HH:mm:ss
a1	[a-zA-Z0-9]	8	32	m	Echo of received a1 parameter.
a4	[0-9]			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 please refer to *Appendix F: Transaction currencies* in the *Source Gateway Payment API* document.
b1	[0-9]	8	19	o	PAN – primary account number (masked)

Field	Type	Min	Max	m/o/c	Comment
b2	[0-9]	1	2	o	Card type. Valid options are: Code Card Scheme 0 Unknown 1 Visa 2 Mastercard 3 American Express 4 Isracard 9 Maestro 10 JCB 12 Discover 13 Diners
b3	[0-9]	2	2	o	Card expiration month Two-digit number, in the format: mm
b4	[0-9]	2	2	o	Card expiration year Two-digit number, in the format: yy
b20	[a-zA-Z0-9]	29	29	o	Payment Account Reference (PAR)
c1	[\ a-zA-Z]	5	50	c (recommended – when initiating 3D secure transaction)	Cardholder's full name Note: the minimum length of this field is five characters. If the cardholder provides a name which is shorter than five characters, you must either add additional non-space characters to the name (e.g. Mr Lu) or not send the field
c3	[a-zA-Z0-9/.@_]	1	127	c	Email address
z1	[a-zA-Z0-9]	1	32	m	Response ID.
z2	[0-9]	1	2	m	Operation result code. Refer to either *Appendix B: Operation Result Codes* in the *Source Gateway Payment API* document, or to *Appendix B: Response Code*.

Field	Type	Min	Max	m/o/c	Comment
z3	[a-zA-Z0-9\-]	1	256	c	Operation result description. Refer to either *Appendix B: Operation Result Codes* in the *Source Gateway Payment API* document, or to *Appendix B: Response Code*.
z4	[a-zA-Z0-9]	1	10	o	Authorisation code.
z6	[A-Z0-9]	1	3	o	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	o	AVS response. The Address Verification Service (AVS) Authorisation response provided by the acquirer at the time of Authorisation. For more information, refer to the Source Gateway Payment API document
z13	[a-zA-Z0-9]	1	32	o	Transaction ID. This identifier should be stored, as 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	o	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 'Y' – CVC1 Incorrect '-' – Not processed

Field	Type	Min	Max	m/o/c	Comment
z15	[0-9]	1	10	o	Approved billing amount, in a 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	o	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. In case such a value is provided by the issuer, it will be returned in this field.
z17	[A-Z]	3	3	o	Balance response currency. In case a balance response is provided (see explanation of field z16), its currency will be returned in this field.
z21	[0-9,-]	1	3	o	Indicates the result of sending the transaction to the Fraud Protection service. See *Appendix C* for the *list of all possible z21 result codes*.
z55	[a-zA-Z0-9]	32	32		Payment ID. A unique transaction identifier that accompanies all transactions related to the same purchase.
d2	text	3	128	o	Echo parameter; if sent with the request, will be returned within the response.
g1	[a-zA-Z0-9]	32	32	o	Token generated by Shift4 in reference to a stored card profile.
payment_method	[a-zA-Z0-9]	1	36	c (will return if this is an APM transaction)	Indicates the selected payment method, which is not credit cards.
c22	[a-zA-Z0-9]	1	11	o (may return if this is an APM transaction)	The BIC number used

Field	Type	Min	Max	m/o/c	Comment
c23	[a-zA-Z0-9]	1	34	o (may return if this is an APM transaction)	The IBAN number used
3ds_status	[A-Z]	1	1	o	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 requests 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_version	[0-9/.]	3	3	o	Indicates whether the 3D secure version is 1.0 or 2.0
3ds_valid_payment	Boolean	1	1	o	Shift4 recommendation whether to initiate payment following the authentication results. Possible values: y – yes n - no
3ds_eci	[0-9]	1	2	o	The ECI assigned to the authentication
3ds_cavv	[a-zA-Z0-9]			o	The authentication value received from the issuer

Field	Type	Min	Max	m/o/c	Comment
3ds_trxid	[a-zA-Z0-9]	36	36	o	The assigned 3D transaction id

Redirect Back

After finishing the processing of the transaction, and once the payment notification response is received (if applicable), Shift4 redirects the shopper back to one of the URLs provided in the original request – 'Success URL' or 'Fail URL' – based on the transaction result.

The redirect operation is signed with a digital signature (K parameter) in order to ensure the information is correct and complete.

We recommend you verify that the redirect URL is correct and complete, and to redirect the shopper only after validation of the digital signature (K parameter).

Appendix A: SHA256 Cipher

To ensure authenticity of the data transfer, every request has a package signature sent as parameter "K". It contains the SHA256 digest 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 alphabetical order (parameters which are capitalised should come first):

   M, O,…, c1, c11, c2, h10, h8, i10, i4,…

2. For each parameter value, replace any special characters < > " ' ( ) \ with spaces.
3. For each parameter value, remove any leading and trailing spaces.
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 of the sorted value set.
7. Include the resulting 32-character string as the "K" parameter in the request.

Signature Calculation Example

The following is an example of calculating the signature using the original request parameters of:

```
M=8632876&O=1&a1=78946541&a4=1099&b1=454545454545454545&b2=1&
b3=08&b4=11&b5=003&c1=John Smith&c3=johnsmith@yahoo.com&c10=AB1
2DE&d1=111.222.0.101
```

1. Sort the parameters:

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

2. For each parameter value, replace any special characters < > "'( ) \ with spaces.
3. For each parameter value, remove any leading and trailing spaces.
4. Line up the values:

   863287617894654110994545454545454545454510811003John SmithAB1 2DEjohnsmith@yahoo.com111.222.0.101

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

   863287617894654110994545454545454545454510811003John SmithAB1 2DEjohnsmith@yahoo.com111.222.0.101SIGNKEY1

6. Calculate the SHA256 of the sorted value set:

   fe0bc19c3a8c532fe2e7671a7a87c16adefa3f175832a1a1b725ce40a5c61dca

7. Include the signature into the request query string:

K=fe0bc19c3a8c532fe2e7671a7a87c16adefa3f175832a1a1b725ce40a5c61dca&M=8632876
&O=1&a1=78946541&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

Response Signature

If a request results in a successful transaction, the Form Payment Page service generates a response signature which can be validated to ensure the authenticity of the response.

To validate the response signature, follow the same steps listed in the section above. Include the response data, append your signature key, but make sure to remove the returned signature.

Appendix B: Response Code

For the full list of 'initiate payment request' response codes and their description, 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 enroled 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.
-36	The selected Processor does not support some of the transaction's parameters.
-35	The selected MID is not registered to your account.
-33	You need to be registered with the routing service to complete the routing request.
-32	You are not registered with the selected Processor.
-31	Authentication process aborted by cardholder.
-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 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
32	Notification timeout, Transaction has been failed.
35	An unexpected error occurred during the APM payment process

Appendix C: z21 Optional Values

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

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

Appendix D: 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 chargeback disputes raised by cardholders and issuers.

Source Payment Gateway offers two modules of 3D Secure:

1. Standard 3D Secure

2. 3DS Adviser – 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 yourself 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. The Source Payment Gateway 3D Secure service automatically selects the correct 3D Secure flow based on the 3D secure protocol supported by the Issuer.

Initiating the 3D Secure process

To initiate the 3D secure process, send the 3ds_initiate parameter as part of the payment request (applicable for operations: Sale, Authorisation and CFT of all types).

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

Value	Description
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 (see *3DS Adviser* for details.)
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 the 3DS Adviser, 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

- You can also choose to only go through the 3D Secure authentication process without actually processing the transaction. To do so use operation code [98] (for further details see the *Source Payment Gateway API* document).

3DS Adviser

The 3DS Adviser module offers a smart recommendation engine that 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 that extends the regular fraud threshold, for authorised 3D secure transactions only.

Name	Type	Min	Max	Description
exemption_action	[0-9]	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	Min	Max	Description
exemption_reason	[0-9]	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.
3ds_tra_score	[0-9]	1	8	Indicates the transaction score value calculated by a third party provider as a basis for *exemption_reason*=01

Additional Response parameters for the 3DS Adviser Module

When using the 3DS Adviser module, additional response parameters are included in the transaction response format:

Name	Type	Min	Max	Description
smart_3ds_result	[0-4]	2	2	Describes the 3DS Adviser module recommendation: 01: Do 3D secure 02: Skip 3D secure 03: Request an exemption as part of the 3D Secure request 04: Request an exemption as part of the payment request
smart_3ds_result_reason	[a-zA-Z0-9]	0	128	Includes the rule id which was executed as part of the Smart 3D rule engine

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 cardholder experience.

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.*

Requested Data	Shift4 Parameters	Description
	c9	Cardholder Billing Address Country Code. Please refer to _ISO 3166-1-alpha-2_ for a list
	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 transaction 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

Name	Description	Type	min	max	m/o/c
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	The Received part of the op code 92 flow. Relevant only if 3ds_channel = 02.	[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_chan nel=01 (APP).
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 a Native UI SDK Interface the accepted values are 01-04, and for an HTML UI the accepted values are 01-05.	Comma separate d list	2	14	c m only when 3ds_chan nel=01 (APP).
3ds_msgextensioni d	A unique identifier for the extension. The Payment System Registered Application Provider Identifier (RID) is required as a prefix of the ID. The maximum length is 64 characters.	[a-zA-Z0-9]	0	64	o
3ds_msgextensinon ame	The name of the extension data set as defined by the extension owner. Maximum length is 64 characters.	[a-zA-Z0-9]	0	64	o

Name	Description	Type	min	max	m/o/c
3ds_msgextensiondata	The data carried in the extension. The maximum length is 8059 characters.	[a-zA-Z0-9]	0	8059	o
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 – Logged in to the cardholder account at the merchant system using merchant's own credentials • 03 – Logged in to the cardholder account at the merchant system using federated ID • 04 – Logged in to the cardholder account at the merchant system using issuer credentials • 05 – Logged in to the cardholder account at the merchant system using third-party authentication • 06 – Logged in 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 cardholder authentication. The 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 carry 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 03 – Optional challenge 04 – Mandatory challenge 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]	0	36	o
3ds_reqpriorauthmethod	Mechanism that was used by the cardholder to previously authenticate to the merchant. Accepted values for this field are: 01- Frictionless authentication performed by the issuer 02 - Cardholder challenged by the issuer 03 - AVS verified 04 - Other issuer methods	[0-4]	2	2	o
3ds_reqpriorauthtimestamp	Date and time in UTC of the prior authentication. Accepted date format is YYYYMMDDHHMM.	[0-9]	12	12	0

Name	Description	Type	min	max	m/o/c
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	2048	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 to 60 days 04 - More than 60 days	[0-4]	2	2	o
3ds_chaccchange	Date that the cardholder's account information 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

Name	Description	Type	min	max	m/o/c
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 to 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 to 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
3ds_nbpurchaseaccount	Number of purchases with this cardholder account during the previous six months.	[0-9]	0	10	o

Name	Description	Type	min	max	m/o/c
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 enroled 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 to 60 days 05 - More than 60 days	[0-5]	2	2	o
3ds_paymentaccage	Date that the payment account was enroled 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; otherwise, it has a value of "false".	[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
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
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. 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
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	128	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	128	o m – when 3ds_addrmatch = false

Name	Description	Type	min	max	m/o/c
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
3ds_shipindicator	Indicates the 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 physical items are included in the sale, specify the relevant shipping code: 01, 02, 03 or 04. If multiple shipping methods are used, specify the shipping method of 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 an 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

Name	Description	Type	min	max	m/o/c
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
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 when the merchandise will be available. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_giftcardamount	For prepaid or gift card purchase, the purchase amount total of prepaid or gift card(s) in major units (for example, USD 123.45 is 123).	[0-9]	1	12	o
3ds_giftcardcurr	For prepaid or gift card purchase, the currency code of the card as defined in _ISO 4217-alpha-3_, except for codes 955 - 964 and 999.	[0-9]	3	3	o
3ds_giftcardcount	For 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

Name	Description	Type	min	max	m/o/c
3ds_recurringexpiry	Date after which no further authorisations will 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
3ds_recurringfrequency	Indicates the minimum number of days between authorisations. The field is limited to a maximum of 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	m
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	o m if 3ds_channel=02
3ds_browserjavaenabled	Boolean that represents the ability of the cardholder browser to execute Java. This field is required for requests where 3ds_channel = 02 (BRW). Accepted values are: true – the cardholder browser can execute Java false - the cardholder browser cannot execute Java	[a-z]	4	5	o m if 3ds_channel=02

Name	Description	Type	min	max	m/o/c
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
d6	Value representing the browser language as defined in IETF BCP47.	[A-Za-z]	1	8	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	o m if 3ds_channel=02
3ds_browserscreenwidth	Total width of the cardholder's screen, in pixels.	[0-9]	1	6	o 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)
d5	Exact content of the HTTP user-agent header.	[a-zA-Z0-9]	5	255	o m if 3ds_channel=02

Name	Description	Type	min	max	m/o/c
3ds_challengewindowsize	Dimensions of the challenge window that will be displayed to the cardholder. The issuer replies with content that is formatted to render in this window so as to provide the best possible user experience. Preconfigured 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 is present when sending to DS, but not present when sending from DS to issuer.	[0-9a-zA-Z]	0	64	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 issuer.	[0-9a-zA-Z]	0	255	o m if 3ds_channel=01
3ds_sdkmaxtimeout	Indicates 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
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

Appendix E: Supported Languages

The following table lists the supported languages that may be sent in the language parameter.

Value	Description
CN	Chinese
DE	German
EN	English (default)
ES	Spanish
FR	French
IT	Italian
PL	Polish
PT	Portuguese
RU	Russian

Change History

Version	Subject/Date	Description
2.6	November 2023	• Rebranded to Shift4
2.5	February 2022	• Added b20 to the Payment Notification Parameters • Changed c1 parameter from optional to recommended
2.4	September 2021	Added possible values to the parameters smart_3ds_result and smart_3ds_result_reason. 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 2	September 2020	• Changed minimum length of a1 parameter • Added an appendix with a list of the supported languages
2.2 rev 1	July 2020	• Changed 3ds_transtype parameter to be mandatory
2.2	May 2020	• Added z55 parameter • Removed 3ds_smarttype & 3ds_smartplan parameters
2.1	June 2019	• Support of 3D secure 2.0
2.0 rev 1	February 2019	• Added support of APMs • Added support of two features: CVV not mandatory for card on file and retry when CVV is wrong.
1.1 rev 4	September 2018	• Removed request_id parameter from the paymentRequest API • Added some clarification about the usage of the op codes • Skin id is mandatory parameter • Changed ShopperID to be shopperID

Version	Subject/Date	Description
1.1 rev 3	August 2018	• Added response code -5
1.1 rev 2	May 2018	• Added BackURL field
1.1	April 2018	• fix in the "paymentRequest" call URL • added information about f21, f22 parameters • added information about the z21 response code • some minor changes in parameters types & descriptions
1.0	October 2017	First release

Support Information

US: +1.617.715.1977

UK: +44.20.3608.1288

EU: +356.2778.0876

Email: support.europe@shift4.com