



API Specifications

Alternative Payment Methods

Version 2.1 rev 2 | May 2024

Contents

Introduction	6
Useful Documents / References	6
API Version Control	6
Certification.....	6
Publisher Information	6
Gateway Interface.....	7
Introduction	7
Uniform Resource Locator (URL) Addresses.....	7
Security/Authentication.....	7
Health Checks.....	7
APM Payment Workflow.....	9
Business Flows	11
General Business Flows.....	11
Business Flows for Specific Payment Methods.....	11
General Message Format.....	13
General.....	13
Headers	13
Body	13
Links	13
Server-2-Server Notification	15
General.....	15
How it works	15
Description of Objects and Fields	16
Root-Level Fields.....	16
Object Name: merchant_info	16
Object Name: amount.....	17
Object Name: purchase_info	17
Object Name: shipping_address.....	17
Object Name: billing_address.....	18
Object Name: shopper_info.....	19
Object Name: redirect_urls.....	21
Object Name: additional_information.....	22
Object Name: payment_details	22

Object Name: seller_information	24
Object Name: threed_secure.....	24
Object Name: exemption.....	29
Object Name: smart_3d.....	30
Object Name: threeds_requestor	31
Object Name: threeds_requestor_authentication_info.....	32
Object Name: threeds_requestor_prior_authentication_info	33
Object Name: purchase	34
Object Name: merchant_risk_indicator	35
Object Name: cardholder_account.....	37
Object Name: acctinfo	37
Object Name: browser_info.....	39
Object Name: sdk.....	41
Object Name: fraud_service	42
Object Name: routing	42
Object Name: result.....	44
Object Name: stand_in_service.....	45
Required Parameters	47
Root-Level Fields	47
Object Name: merchant_info	47
Object Name: amount.....	47
Object Name: purchase_info	48
Object Name: shipping_address.....	48
Object Name: billing_address.....	49
Object Name: shopper_Info.....	50
Object name: additional_information	52
Object name: redirect_urls	52
Object Name: seller_information	53
Object Name: threed_secure.....	54
Object name: payment_details.....	55
Response Message Format	56
Object Name: purchase_info	56
Object Name: shopper_info.....	57
Object Name: result.....	57
Object Name: stand_in_service.....	58

Object Name: amount.....	58
Object Name: links.....	59
Object Name: additional_information.....	59
Object name: redirect_urls.....	59
Object name: payment_details.....	60
Object name: payment_details.fraud.....	61
Object name: routing.....	61
Object Name: threed_secure.....	62
Retrieval (GET) Transaction Format Purpose.....	65
GET Banks API.....	67
Request parameters.....	67
Response Format.....	67
PayPal Specifications.....	69
Special Processing Requirements.....	69
Specific Processing Rules & Disclaimers.....	74
Branding.....	75
Apple Pay Specifications.....	76
Apple Pay integration.....	76
Registration with Apple.....	76
Transaction flow.....	77
Google Pay Specifications.....	78
Google Pay integration.....	78
Transaction flow.....	78
MobilePay Specifications.....	80
How to prepare for processing MobilePay.....	80
Sale Transaction Flow.....	80
Payout.....	81
Additional Request Parameters for Specific Payment Methods.....	82
Object Name: payment_details.....	82
Object Name: recipient_info.....	84
Object Name: redirect_urls.....	85
Object Name: routing.....	85
Object Name: fraud.....	86
Object Name: browser_info.....	86
Object Name: device_info.....	86

Appendix A: SHA512 Transaction Signature	88
Appendix B: Operation Result Codes	89
Appendix C: Available Payment Methods.....	91
Appendix D: SCA & 3D Secure.....	95
3D Secure and Customer Experience: Frictionless Experience vs. Cardholder Challenge.....	95
3D Secure Transaction Flow.....	96
Strong Customer Authentication (SCA)	104
Smart 3D Secure Standalone Services	122
Appendix E: How to Provide 3D Secure Authentication Data	124
ECI (Electronic Commerce Indicator)	124
CAVV/AAV and XID.....	125
Guidelines for 3D secure 2.0 and higher.....	127
Appendix F: Setting Up MobilePay	128
Revision History	129
Need Support?	135

Introduction

The purpose of this document is to provide an in-depth description of *Shift4's* Alternative Payment Methods (APM) Gateway API. *Shift4's* APM Gateway is a proprietary platform for processing Alternative Payment Method transactions.

The APM API is a simple-to-use RESTful API. The API operates as a basic request-response service where the client instructs the gateway to perform an operation and the gateway replies with the operation's status. There are, however, situations where the merchant will have to carry out a follow-up action in order to complete the transaction.

Useful Documents / References

The following documents may also be useful in understanding the *Shift4* API:

- *Shift4 Payment API*: an in-depth description of *Shift4's* Payment Gateway API.
- *Shift4's Hosted Payment Page API*: an in-depth description of *Shift4's* Hosted Payment Page services solution.
- *Shift4's Data Transfer Interface*: an in-depth description of the ePower Data Transfer Interface that lists the available reports' formatting specifications.

These documents can be found on the [Shift4 Developer Portal](#).

API Version Control

The information provided in this document is accurate and reliable for standard processing as of its publication date. Any new implementations should thus avoid using previous versions of the API specification.

The API version number is a sequence-based identifier. Changes to the first part thus indicate major specification updates, while changes to the second part indicate minor updates.

The revision number reflects smaller specification changes, the correction of typing errors, or corrections that do not affect the API protocol itself.

Certification

All new implementations must go through a certification process in order to ensure the quality of their integrations and the integrity of merchant data.

An additional certification process will be required if new operation codes or features are introduced.

Publisher Information

Copyright © *Shift4*. All rights reserved.

Gateway Interface

Introduction

Transaction requests are sent online and in real-time using the HTTPS (Hypertext Transfer Protocol - Secure) protocol. The Gateway protocol, in turn, exposes multiple operation types, including sale (Authorisation and Capture), Authorisations, Reversals, Refunds and Past Transaction Enquiries.

Uniform Resource Locator (URL) Addresses

Integration URL	https://pay.int.sourcepayments.com/payments/rest
Production URL	https://pay.sourcepayments.com/payments/rest

Security/Authentication

All HTTP requests must be sent over a secure TLS (Transport Layer Security) 2.0 channel. The *Shift4* APM Gateway does not authenticate the TLS/SSL (Secure Sockets Layer) session using a client-based certificate, and thus does not employ a regular type of session authentication. Instead, the client is first authenticated by its source IP alongside a secondary authentication check that employs a cipher sent in the request header and used for pre-processing verifications. See [Appendix A: SHA512 Transaction Signature](#) for further details.

Health Checks

The health of the *Shift4* Alternative Payment Methods Gateway and Integration Environments can be checked by accessing the following URLs:

Production		
Production Environment	Payment Server	https://pay.sourcepayments.com/rest/health
Production Environment	Notification Server	https://notification.sourcepayments.com/rest/health

Integration		
Integration Environment	Payment Server	https://pay.int.sourcepayments.com/rest/health
Integration Environment	Notification Server	https://notification.int.sourcepayments.com/rest/health

The service will then respond with a JavaScript Object Notation (JSON) message. One of the following responses will be provided:

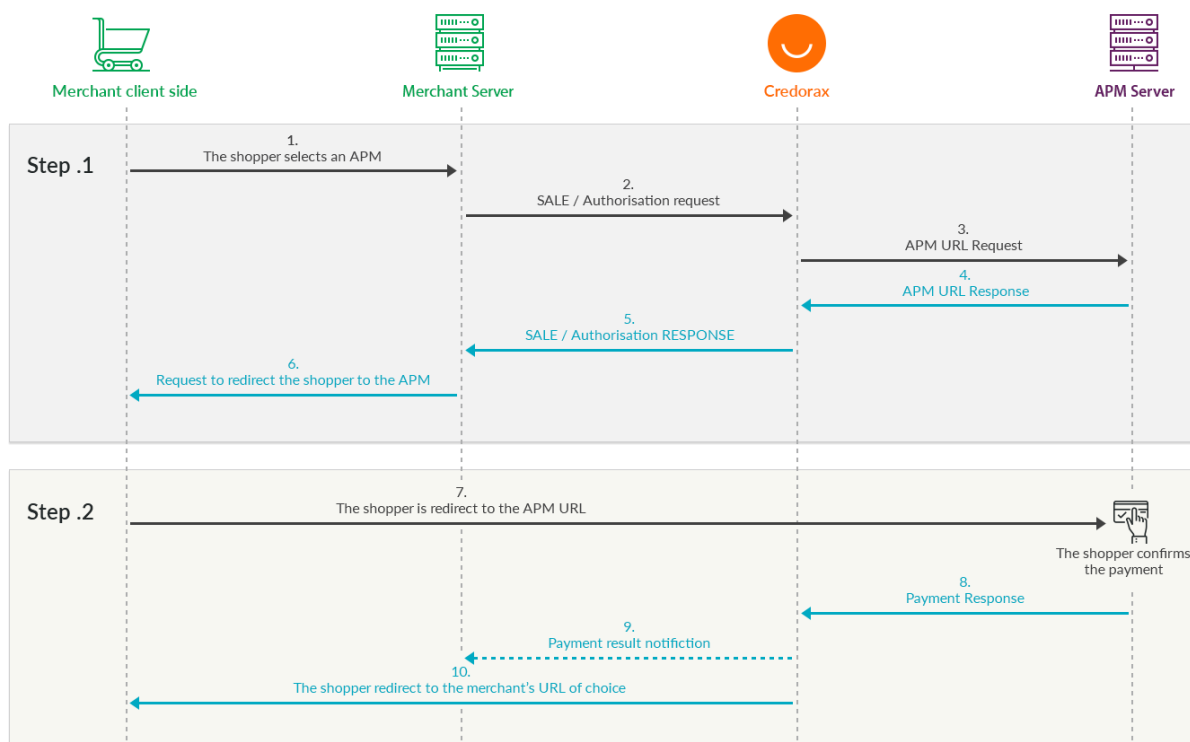
- `{"health":"OK"}`

- {"health":"FAIL"}

Follow the following guidelines when using this service:

- A **maximum** of one health check is permitted every 10 seconds
- A time-out should be recorded if no response has been received within 20 seconds
- The *Shift4* processing service should be considered unavailable after 3 consecutive service failures
- Please contact the Shift4 Support Team immediately in the event of any unexpected service interruption at support.europe@shift4.com

APM Payment Workflow



Step 1

1. The shopper selects the APM they wish to use in order to complete the checkout on the merchant's website.
2. The merchant initiates a call, typically a **Sale** API request; if the APM supports an Authorisation and Capture flow, the call could involve separate **Authorisation** and **Capture** API requests. These requests, in turn, would contain all the payment-related information. Furthermore, the most important parameters in this request are the *payment_method* and *redirect_urls* objects (For further information, see the [Objects & Fields](#) chapter).
3. *Shift4* routes the payment to the requested Payment Method and returns a URL to which the merchant must redirect the shopper. If the shopper is not redirected to this URL, the payment cannot be completed and no funds will be transferred to the merchant's account.

Step 2

1. The payment process is completed only after the shopper has confirmed the payment at the payment URL. *Shift4* then redirects the shopper to the merchant landing page specified in the applicable *redirect_urls* object URL.
2. *Shift4* then sends the merchant a webhook (optionally) with the payment's result. The merchant can refund this payment if necessary by using the link specified in the webhook it just received.

Synchronous Flow

There are some APMs that behave in single, synchronous request-response flow. For those APMs, Step 1 returns a final, absolute answer, and the entire Step 2 is not performed.

Business Flows

The *Shift4* APM Gateway supports the following business operations:



Note:

Each payment method supports specific business flows.

General Business Flows

Sale

A Sale request performs both Authorisation and Capture transactions at the same time, i.e. sends an Authorisation request to the shopper's account and Captures the funds immediately upon its approval.

Refund

A Refund is the decline of a previously Captured transaction (or Sale transaction). A Refund request can be sent up to 180 days from the relevant transaction's Date of Capture.



Note:

Refer to [Appendix C: Available Payment Methods](#) for payment methods that support refunds

Retrieval Call (GET)

A Retrieve Call operation retrieves information regarding a previous transaction. This call can be initiated for any type of transaction.

Business Flows for Specific Payment Methods

Authorisation

An API call that generates an online Authorisation request.

An authorisation (auth) request is sent from a merchant portal (such as a website, mobile phone or Interactive Voice Response (IVR) service) to the Gateway in order to verify that sufficient funds are available and reserved for settling the payment transaction in due time.

Capture

A capture request causes the transfer of funds from the shopper's account to the merchant's account. This transaction is always performed after an auth transaction. Note that an Authorisation

transaction does not guarantee the transfer of funds to a merchant unless it is followed by a capture transaction.

NOTE	Capture requests are only supported by PayPal, Apple Pay and Google Pay.
------	--

Re-Authorisation

A re-authorisation request extends the timeframe during which funds are guaranteed to the merchant after a Capture transaction.

NOTE	Re-authorisation requests are only supported by PayPal.
------	---

Authorisation Void

A Void request causes the cancellation of an authorised transaction and the release of the funds reserved during the Auth request.

NOTE	Void requests are only supported by PayPal, Apple Pay and Google Pay
------	--

Payout

A Payout request initiates funds movement from the merchant account to the shopper account.

NOTE	Payout is currently supported only by Apple Pay, Google Pay and MobilePay. Payout for these payment methods is processed as a referral transaction that refers to a previous original transaction, and relies on the information sent in the original transaction.
------	--

General Message Format

General

The *Shift4* APM API is a JSON-formatted REST API.

The request type is sent as part of the gateway URL.

For example:

```
.../payments/rest/sale
```

```
.../payments/rest/authorize
```

Headers

Authentication header: contains the hashed string that signs the request. See [Appendix A: SHA512 Transaction Signature](#) for more information.

Content-Type: application/json

Example:

Authentication: Bearer A21AAGqwTe-vsPxp3DislZ5siOrfyaj0bTsRi7NqK3SJWxSvMs_tgK-L7AGHdLW7BZXttjPFDcl9ajpfI03EO2z_LUskR5E2g

Content-Type: application/json

Body

Valid JSON message. For more details about the possible objects and attributes in a message, see the [Description of Objects and Fields](#) chapter.

Links

The *Shift4* APM API calls return a result code and relevant descriptions. Some API calls also return JSON response bodies that include information about the resource, including one or more contextual HATEOAS links (“Links” objects). It is recommended that these links be used for requesting more information and for constructing an API flow that is suited to a particular request. The following table explains how you can build the destination URLs yourself:

Required Operation	URL format
Capture (for	.../payments/rest/capture/{sub_merchant_id*}/{original_transaction_id}
Void)	.../payments/rest/void/{sub_merchant_id*}/{original_transaction_id}
Refund	.../payments/rest/refund/{sub_merchant_id*}/{original_transaction_id}

Required Operation	URL format
Re-authorisation	.../payments/rest/re-Authoisation/{sub_merchant_id*}/{original_transaction_id}
Payout	.../payments/rest/payout/{sub_merchant_id*}/{original_transaction_id}

NOTE

If not required, there is no need to fill in the sub merchant id value.
Some of these request types are only supported by certain payment methods

Server-2-Server Notification

General

APM flows are based on a two-step process requiring shopper action, *Shift4* payments platform supports an automated notification to update about the transaction's status after the shopper's action.

We strongly recommend you implement this notification functionality to support your business flow.

NOTE	To set up the notification functionality contact your Solution Architect and provide the URL to which you wish to receive the notifications
------	---

How it works

- The gateway will send the notification and will immediately redirect the shopper's browser to the relevant URL.
- The gateway expects to receive a "200: OK" response from the shopper's browser

The gateway will retry sending the notification in a 15 minutes interval, and a maximum of 192 retries, until a successful HTTP response message (200:OK) is received.

You can also transmit a GET request to in order to query a transaction if you wish to get an update on this transaction without waiting for the automatic notifications.

Notification Format

The notification format is similar to the Sale/Authorisation response format.

IP Whitelisting

In order to receive notifications in Production environment make sure to whitelist the following IP on your system: 199.233.202.0/23

Description of Objects and Fields

This chapter describes all the API objects and fields. Refer to the [Required Parameters Chapter](#) for a mapping of mandatory/optional parameters according to different business use cases

NOTE field names are case-sensitive.

Root-Level Fields

Parameter Name	Type	Min	Max	Description
request_id	[a-zA-Z0-9]	8	32	Merchant-generated unique Request ID
payment_method	[a-zA-Z0-9]	4	20	The selected Payment Method. See the available options in Appendix C- Available Payment Methods
payment_id	[a-zA-Z0-9]	16	32	<i>Shift4</i> -generated unique Payment ID. Connects all the transactions associated with the same payment.
reference_transaction_id	[a-zA-Z0-9]	16	32	The transaction ID in question
create_token	[a-z]	4	5	Indicates whether a token should be created. Accepted values are: <ul style="list-style-type: none"> true false

Object Name: merchant_info

Field Name	Type	Min	Max	Description
gw_mid	[a-zA-Z0-9]	3	8	The <i>Shift4</i> gateway Merchant ID
descriptor	[a-zA-Z0-9]	0	22	The business descriptor that appears on the shopper's payment statement
sub_merchant_id	[a-zA-Z0-9]	1	15	The sub-merchant ID
reference_number	[a-zA-Z0-9]	1	32	Merchant Reference Number. This optional field is a secondary Transaction Reference Number which can be transmitted to add another identifier of the transaction. Note: No cardholder data should be provided in this field.

Object Name: amount

Field Name	Type	Min	Max	Description
amount	[a-zA-Z0-9]	1	10	The requested Billing Amount Two exponents without a decimal are implied apart from currencies with zero exponents. For example, a value of 1000 should be transmitted for an amount of 10.00 GBP, but a value of 10 should be transmitted for an amount of 10 JPY.
currency	3 character ISO 4217-alpha-3 currency code	3	3	Transaction currency. Indicates the currency that should be used in the transaction. NOTE: Every currency you wish to use must be preconfigured on the Shift4 payments platform.

Object Name: purchase_info

Field Name	Type	Min	Max	Description
free_field	[a-zA-Z0-9]	0	127	Free field for the merchant's use
purchase_order	[a-zA-Z0-9]	0	127	The purchase order number or ID. Identifies this payment.
description	[a-zA-Z0-9]	0	127	Description of the purchase
invoice_number	[a-zA-Z0-9]	0	127	Purchase invoice number
mobile_view	Boolean (true/false)	4	5	Indicates if mobile variant of a scheme is enabled
number_of_items	[0-9]	1	2	the number of items purchased
discount_code	[a-zA-Z0-9]	1	12	The discount code used in the purchase

Object Name: shipping_address

Field Name	Type	Min	Max	Description
line_1	[a-zA-Z0-9]	4	64	The shopper's Shipping Address

Field Name	Type	Min	Max	Description
line_2	[a-zA-Z0-9]	4	64	The second line of the address. This could include a suite, an apartment number, and so on.
country_code	two-character ISO-3166-1 country codes	2	2	The shipping address' country code
city	[a-zA-Z0-9]	4	32	The shopper's city as noted in the shipping address
phone_number	[0-9,-]	4	50	The shopper's phone number
state	[a-zA-Z0-9]	2	40	The state code,. Required for transactions if the shipping address is in one of the following countries: Argentina, Brazil, Canada, India, Italy, Japan, Mexico, Thailand, or United States. The maximum length is 40 single-byte characters.
postal_code	[a-zA-Z0-9]	2	16	The shipping address' postal code
shipping_method	[a-zA-Z0-9]	1	32	The shipping method used for this purchase
shipping_class	[a-zA-Z0-9]	1	32	The shipping class
expected_delivery_date	DATE	8	8	The expected delivery date

Object Name: *billing_address*

Field Name	Type	Min	Max	Description
line_1	[a-zA-Z0-9]	4	64	The shopper's billing address, including street name and number
line_2	[a-zA-Z0-9]	4	64	The second line of the billing address.
country_code	two-character ISO-3166-1 country codes	2	2	The billing address' country code

Field Name	Type	Min	Max	Description
city	[a-zA-Z0-9]	4	32	The billing address city
phone_number	[0-9]	4	50	The billing address phone number
state	[a-zA-Z0-9]	2	40	The state code or name. Required for transactions if the address is in one of the following countries: Argentina, Brazil, Canada, India, Italy, Japan, Mexico, Thailand, or the United States. The maximum length is 40 single-byte characters.
postal_code	[a-zA-Z0-9]	2	16	The billing address' postal code

Object Name: shopper_info

Field Name	Type	Min	Max	Description
country_code	two-character ISO-3166-1 country codes	2	2	The shopper's country code
birth_date	[0-9,-]	3	32	The shopper's date of birth in YYYY-MM-DD format.
last_name	[a-zA-Z0-9]	3	32	The shopper's last name. Note: If the shopper's last name is shorter than three characters, you must add additional characters
shopper_id	[a-zA-Z0-9]	4	128	The specific payment method's shopper ID
phone_number	[0-9,-]	4	32	The shopper's personal phone number
mobile_phone	object	-	-	The shopper's personal mobile phone number. Constructed from two parts: <ul style="list-style-type: none"> number country For example: <pre>"mobile_phone": { "number": "51111111", "country": "111" }</pre>

Field Name	Type	Min	Max	Description
home_phone	Object	-	-	<p>The shopper's home phone number. Constructed from two parameters:</p> <ul style="list-style-type: none"> number country: 3-digit numeric country code <p>For example:</p> <pre>"home_phone": { "number": "51111111", "country": "111" }</pre>
work_phone	Object	-	-	<p>The shopper's work phone number. Constructed from two parameters:</p> <ul style="list-style-type: none"> number country: 3-digit numeric country code <p>For example:</p> <pre>"work_phone": { "number": "51111111", "country": "111" }</pre>
ip_address	[a-zA-Z0-9]	7	15	The IP address of the device the shopper is using to initiate the purchase
first_name	[a-zA-Z0-9]	3	32	The shopper's first name. If shorter than three characters, you must add additional characters
email	[a-zA-Z0-9]	3	127	The shopper's email address
language	[a-z]	2	2	The 2-letter language code (e.g. en for English) that should be preferred when presenting payment pages to the consumer
bic	[a-zA-Z0-9]	8	11	BIC (bank identification code)
iban	[a-zA-Z0-9]	30	34	Consumer bank account IBAN
personal_id	[a-zA-Z0-9/-]	8	16	The end-user's personal identification number (e.g. social security number, identification number, birth number). Useful for some banks for identifying

Field Name	Type	Min	Max	Description
				transactions and for KYC/AML purposes.
id_type	[A-Z]	1	4	Beneficiary's personal identification type. Possible values depend on buyer's country: <ul style="list-style-type: none"> Colombia possible values: <ul style="list-style-type: none"> CC (citizen identification document), CE (foreigner identification document), PASS (passport) NIT (Tax number) Peru possible values: <ul style="list-style-type: none"> DNI (Identification document) RUC (Tax number) CE foreigner identification document) PASS(Passport)
bank_code	[a-zA-Z]	3	3	The bank code of the selected bank for the transfer See more details in the GET Banks API

Object Name: *redirect_urls*

Field Name	Type	Min	Max	Description
success_url	URL	0	1024	The URL to which the user is redirected in case of a successful transaction
cancel_url	URL	0	1024	The URL to which the user is redirected in case of a cancelled transaction

Field Name	Type	Min	Max	Description
fail_url	URL	0	1024	The URL to which the user is redirected in case of a failed transaction
pending_url	URL	0	1024	The URL to which the user is redirected in case of a pending transaction
redirect_url	URL	0	2048	Received in the response message and indicates to which URL to redirect the shopper. Contains one of the following values: <ul style="list-style-type: none"> From a payment method: The URL to which the user is redirected in order to complete the purchase From the issuer (for 3D Secure): The issuer's URL for the 3D secure authentication process
redirect_url_app	URL	0	2048	Received in the response message and indicates to which mobile application URL to redirect the shopper in case the shopper should be redirected to the payment method's application

Object Name: additional_information

Field name	Type	Min	Max	Description
account_type	[a-z]	1	1	The type of account. Possible values: C: for Current accounts S: for Savings accounts I: International accounts
bank_branch	[a-zA-Z0-9]	1	45	Shopper's bank branch name

Object Name: payment_details

Field name	Type	Min	Max	Description
pan	[0-9]	8	19	PAN – Primary Account Number
expiry_month	[0-9]	2	2	Card expiration month in two-digit format (mm)
expiry_year	[0-9]	2	2	Card expiration year in two-digit format (yy)
authorization_code	[a-zA-Z0-9]			Authorisation Code
rrn	[0-9]	1	10	The transaction's Retrieval Reference Number (RRN). The RRN may be provided by the processor as an additional identifier of the transaction. Every refund transaction will receive a unique RRN, different from the initial transaction RRN.
initial_transaction_id	[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'.
fast_funds_indicator	[A-Z]	1	1	Fast funds indicator. Indicates whether the issuer supports fast funds functionality. Possible values are: Y – Supports fast funds for domestic & cross-border payments C – Supports fast funds for cross-border payments D – Supports fast funds for domestic payments N – No result
recurring	[A_Z]	5	10	Indicates whether the transaction is the first of a recurring series of payments or a subsequent payment in the series. Possible values: • FIRST • SUBSEQUENT
token	JSON	0	4096	Used for the following:

Field name	Type	Min	Max	Description
				<ul style="list-style-type: none"> The token created if the <code>create_token</code> parameter was used The assigned payment token for mobile payments.
<code>partial_capture_indicator</code>	[a-z]	4	5	Partial capture indicator Accepted values: <ul style="list-style-type: none"> true false Used with Israeli processors only
<code>cardholder_name</code>	[a-zA-Z0-9]	3	32	Cardholder full name

Object Name: `seller_information`

This object is required for marketplaces, to provide information about the seller fulfilling the transaction

Field name	Type	Min	Max	Description
<code>id</code>	[a-zA-Z0-9_-]	4	64	The seller's ID. The ID should be a unique identifier such as the seller name or an internal registration number.
<code>country</code>	[A-Z]	3	3	The seller's country.
<code>city</code>	[a-zA-Z_-]	3	30	The seller's city.
<code>line_1</code>	[a-zA-Z0-9_-]	4	50	The seller's address.
<code>postal_code</code>	[a-zA-Z0-9_-]	1	9	The seller's postal code.
<code>state</code>	[a-zA-Z0-9]	3	3	The seller's state.

Object Name: `threed_secure`

Field name	Type	Min	Max	Description
<code>threeds_status</code>	[A-Z]	1	1	The result of the authentication process. Possible values: A – Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted

Field name	Type	Min	Max	Description
				<p>authentication/verification is provided</p> <p>Y – Authentication/ Account Verification Successful</p> <p>N – Not Authenticated /Account Not Verified; Transaction denied</p> <p>C – Challenge Required; Additional authentication is required</p> <p>R – Authentication/ Account Verification Rejected; Issuer is rejecting authentication/verification and requests that authorisation not be attempted.</p> <p>U – Authentication/ Account Verification Could Not Be Performed, Technical or other problem</p> <p>I – Informational Only; Merchant challenge preference acknowledged.</p> <p>D – Challenge Required; Decoupled Authentication confirmed</p>
valid_payment	[yn]	1	1	<p>Shift4 recommendation whether to initiate payment following the authentication results. Possible values:</p> <p>y – yes</p> <p>n – no</p>
initiate	[0-4]	2	2	<p>Indicates whether to initiate the Shift4 3D Secure Authentication process. Possible values are:</p> <p>01: Initiate 3D Secure before completing the payment</p> <p>02: Process payment without initiating 3D Secure</p> <p>03: Initiate 3D Secure according to the 3DS Adviser result (see 3DS Adviser)</p>

Field name	Type	Min	Max	Description
				For additional information about the 3D Secure process, see Appendix D: SCA & 3D Secure . Note: If the transaction contains all the following parameters, it will be declined: <code>threed_secure.initiate</code> , <code>threed_secure.eci</code> and <code>threed_secure.cavv</code> .
trxid	[a-zA-Z0-9]	36	36	The assigned 3D transaction ID
channel	[0-3]	2	2	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)
category	[0-3]	2	2	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 threed_secure.channel = 01 or 02)
completion_ind	[Y,N,U]	1	1	Relevant only if threed_secure.channel = 02. Received as part of the 3DS completion flow. The accepted values are: Y – Successfully completed N – Did not successfully complete U – Unavailable
redirect_url	URL	0	2048	The merchant URL to which the browser should be redirected after the challenge session
merchant_name	String	4	40	The 3DS merchant name as assigned by the acquirer

Field name	Type	Min	Max	Description
acquirer_bin	Numeric	6	12	The acquirer BIN number
acquirer_password	String	4	32	The 3D Secure authentication password as assigned by the acquirer
acquirer_mid	String	4	32	The 3D Secure merchant ID as assigned by the acquirer
merchant_url	URL	4	256	The merchant URL (website)
merchant_country	Numeric	3	3	The merchant country as a 3-digit numeric country code
merchant_mcc	Numeric	4	4	The merchant category code (MCC) as assigned by the acquirer
requestor_id	Alphanumeric	0	35	The unique 3D Secure requestor id. Depends on whether you are: <ul style="list-style-type: none"> Providing 3DS Standalone to Multiple Merchants Using 3DS Standalone as a Single Merchant
requestor_name	Alphanumeric	0	40	The unique 3D Secure requestor name. Depends on whether you are: <ul style="list-style-type: none"> Providing 3DS Standalone to Multiple Merchants Using 3DS Standalone as a Single Merchant
version	[0-9]	3	5	Indicates the 3D Secure protocol version. Possible values: <ul style="list-style-type: none"> 1.0 2.0 2.1.0 2.2.0
thredsmethod	URL	-	-	The issuer's URL that should be used to trigger the collection of the device fingerprint by the issuer
cavv	[a-zA-Z0-9]	0	64	The authentication value received from the issuer

Field name	Type	Min	Max	Description
eci	[0-9]	1	2	The ECI assigned to the authentication
xid	[a-zA-Z0-9]	28	28	XID generated as part of the authentication. Relevant only for 3D Secure version 1.0.2
dstrxid	[0-9A-Za-z,-]	34	34	3DS Directory server transaction ID. Must be sent if threed_secure.version = 2.0 or higher and threed_secure.eci, threed_secure.cavv are used. Refer to Appendix E: How to provide 3D secure Authentication Data
pareq	[a-zA-Z0-9]	0	2048	Relevant only for 3D secure 1.0 flows. Used when accessing the redirect_urls.redirect_url
acstansid	[a-zA-Z0-9\,-]	36	36	Unique transaction identifier assigned by the ACS to identify a single 3D secure transaction.
white_list_status	[A-Z]	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
exemption	Object	-	-	See the exemption object
smart_3d	Object	-	-	See the smart_3d object
threeds_requestor	Object	-	-	See the threeds_requestor object
cardholder_account	Object	-	-	See the cardholder_account object
purchase	Object	-	-	See the purchase object
sdk	Object	-	-	See the sdk object

Object Name: exemption

Field name	Type	Min	Max	Description
action	[0-9]	2	2	<p>Indicates the merchant preference regarding SCA exemption. Possible values are:</p> <p>01: Do not request exemption. This is the default behaviour for the Shift4 Gateway. If the field is absent from the transaction request, no exemption will be applied.</p> <p>02: Request an exemption as part of the payment request.</p> <p>03: Request an exemption as part of the 3D Secure request</p> <p>04: Request exemption by default. Shift4 will apply for exemption as part of the 3D Secure request if possible.</p> <p>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.</p>
reason	[0-9]	2	2	<p>This field is required when exemption.action= 02 or 03.</p> <p>Possible values:</p> <p>01: Low value transaction (below 30 EUR or equivalent)</p> <p>02: Low risk transaction (TRA)¹</p> <p>03: Request Trusted Beneficiary Indicator (Whitelisting)²</p> <p>04: Secure Corporate Cards³</p> <p>05: Delegated Authentication⁴</p> <p>06: MIT – Recurring same amount</p> <p>07: MIT – other⁵</p> <p>08: Trusted Beneficiary Indicator (Whitelisting) – Done⁶</p>

Field name	Type	Min	Max	Description
				<p>¹ Requires real-time fraud monitoring solutions</p> <p>² Use this value to indicate to the ACS to obtain confirmation from the cardholder to whitelist the merchant for future purchases</p> <p>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.</p> <p>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.</p> <p>⁵ Any MIT transaction must be sent with this flag to make sure the transaction will not require SCA.</p> <p>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.</p>
TRA_score	[0-9,AZa-z]	1	8	Indicates the transaction risk analysis result calculated by a third party provider as a basis for exemption. reason=02

Object Name: smart_3d

Field name	Type	Min	Max	Description
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
result_reason	[a-zA-Z0-9]	0	128	Includes the rule id which was executed as part of the Smart 3D rule engine

Object Name: threads_requestor

Field name	Type	Min	Max	Description
threads_requestor_challenge_in d	[0-4]	2	2	Indicates whether a challenge is requested for this transaction. For example: For thread_secure.category 01-PA, a merchant may have concerns about the transaction, and request a challenge. For thread_secure.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

Field name	Type	Min	Max	Description
				08 - No challenge requested (utilise whitelist exemption if no challenge required) 09 - Challenge requested (whitelist prompt requested if challenge required)
threads_requestor_dec_req_ind	[YN]	1	1	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.
threads_requestordec_max_time	[0-9]	1	5	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.
threads_requestor_authentication_info	Object	-	-	See the threads_requestor_authentication_info object
threads_requestor_prior_authentication_info	Object	-	-	See the threads_requestor_prior_authentication_info object

Object Name: threads_requestor_authentication_info

Field name	Type	Min	Max	Description
threads_req_auth_method	[0-6]	2	2	Information about how the cardholder was authenticated before or during the transaction.

Field name	Type	Min	Max	Description
				<p>The mechanism used by the Cardholder to authenticate to the merchant. Accepted values are:</p> <ul style="list-style-type: none"> • 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)
threads_req_auth_timestamp	[0-9]	12	12	Date and time in UTC of the cardholder authentication. Field is limited to 12 characters and the accepted format is YYYYMMDDHHMM
threads_req_auth_data	[a-zA-Z0-9]	0	255	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.

Object Name: threads_requestor_prior_authentication_info

Field name	Type	Min	Max	Description
threads_req_prior_ref	[a-zA-Z0-9]	36	36	This data element provides additional information to the issuer to determine the best approach for handling a request. The

Field name	Type	Min	Max	Description
				element contains the issuer's Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the cardholder).
threads_req_prior_auth_method	[0-4]	2	2	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
threads_req_prior_auth_timestamp	[0-9]	12	12	Date and time in UTC of the prior authentication. Accepted date format is YYYYMMDDHHMM.
threads_req_prior_auth_data	[a-zA-Z0-9]	0	2048	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.

Object Name: purchase

Field name	Type	Min	Max	Description
merchant_risk_indicator	Object	-	-	See the merchant_risk_indicator object
purchase_date	[0-9]	14	14	Date and time of the purchase expressed in UTC. The field is formatted as YYYYMMDDHHMMSS.
recurring_expiry	[0-9]	8	8	Date after which no further authorisations shall be performed. This field is limited to 8 characters, and the accepted format is

Field name	Type	Min	Max	Description
				YYYYMMDD. This field is required if payment_details.recurring=1 or 2
recurring_frequency	[0-9]	0	4	Indicates the minimum number of days between authorisations. The field is limited to 4 characters. This field is required if payment_details.recurring=1 or 2
trans_type	[0-9]	2	2	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

Object Name: merchant_risk_indicator

Field name	Type	Min	Max	Description
ship_indicator	[0-7]	2	2	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 threed_secure.cardholder.addr_match = true. 03 - Ship to address that is different from the cardholder's billing address. In this case, shipping information is required even though threed_secure.cardholder.addr_match = true. 04 - "Ship to Store" / Pick-up at local store (store address is populated in the shipping address fields). In

Field name	Type	Min	Max	Description
				<p>this case, shipping information is required even though <code>threed_secure.cardholder.addr_match = true</code>.</p> <p>05 - Digital goods (includes online services, electronic gift cards and redemption codes)</p> <p>06 - Travel and Event tickets, not shipped</p> <p>07 - Other (for example, Gaming, digital services not shipped, emedia subscriptions, etc.)</p>
delivery_timeframe	[0-4]	2	2	<p>Indicates the merchandise delivery timeframe.</p> <p>Accepted values are:</p> <p>01 - Electronic Delivery</p> <p>02 - Same day shipping</p> <p>03 - Overnight shipping</p> <p>04 - Two-day or more shipping</p>
delivery_email_address	Email	7	64	<p>For electronic delivery, the email address to which the merchandise was delivered.</p>
reorder_items_ind	[0-2]	2	2	<p>Indicates whether the cardholder is reordering previously purchased merchandise. Accepted values are:</p> <p>01 - First time ordered</p> <p>02 - Reordered</p>
preorder_purchase_ind	[0-2]	2	2	<p>Indicates whether the cardholder is placing an order for merchandise with a future availability or release date.</p> <p>Accepted values are:</p> <p>01 - Merchandise available</p> <p>02 - Future availability</p>
preorder_date	[0-9]	8	8	<p>For a pre-ordered purchase, the expected date that the merchandise will be available.</p> <p>Date format must be YYYYMMDD.</p>
gift_card_amount	[0-9]	1	12	<p>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).</p>
gift_card_curr	[0-9]	3	3	<p>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.</p>

Field name	Type	Min	Max	Description
gift_card_count	[0-9]	0	2	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.

Object Name: *cardholder_account*

Field name	Type	Min	Max	Description
acctinfo	Object	-	-	See the acctinfo object
acc_id	[a-zA-Z0-9]	0	64	Additional information about the account optionally provided by the merchant
pay_token_ind	[a-z]	4	5	This field has a value of "true" if the transaction was de-tokenised prior to being received by Shift4.
addr_match	[a-z]	4	5	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical. Accepted values: <ul style="list-style-type: none"> • True - Shipping Address matches Billing Address • False - Shipping Address does not match Billing Address Note: the default value of this field is 'false'

Object Name: *acctinfo*

Field name	Type	Min	Max	Description
chacc_date	[0-9]	8	8	Date that the cardholder opened the account with the merchant. Date format = YYYYMMDD.
chacc_change_ind	[0-4]	2	2	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: <ul style="list-style-type: none"> 01 - Changed during this transaction 02 - Less than 30 days 03 - 30 - 60 days 04 - More than 60 days

Field name	Type	Min	Max	Description
chacc_change	[0-9]	8	8	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.
chacc_pw_change_ind	[0-5]	2	2	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
chacc_pw_change	[0-9]	8	8	Date that cardholder's account with the merchant had a password change or account reset. Date format must be YYYYMMDD
ship_address_usage_ind	[0-4]	2	2	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
ship_address_usage	[0-9]	8	8	Date when the shipping address used for this transaction was first used. Date format must be YYYYMMDD.
txn_activity_day	[0-9]	0	10	Number of transactions (successful and abandoned) for this cardholder account with the merchant across all payment accounts in the previous 24 hours.
txn_activity_year	[0-9]	0	10	Number of transactions (successful and abandoned) for this cardholder account with the merchant across all payment accounts in the previous year.
provision_attempts_day	[0-9]	0	10	Number of Add Card attempts in the last 24 hours.
nbpurchase_account	[0-9]	0	10	Number of purchases with this cardholder account during the previous six months

Field name	Type	Min	Max	Description
suspicious_acc_activity	[0-2]	2	2	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
ship_name_indicator	[0-2]	2	2	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
payment_acc_ind	[0-5]	2	2	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
payment_acc_age	8	8	[0-9]	Date that the payment account was enrolled in the cardholder's account with the merchant. Date format must be YYYYMMDD.

Object Name: browser_info

Field name	Type	Min	Max	Description
browser_java_script_enabled	[a-z]	4	5	Boolean that represents the ability of the cardholder browser to execute JavaScript. Accepted values are true / false
browser_java_enabled	[a-z]	4	5	Boolean (true/false) that represents the ability of the cardholder browser to execute Java. This field is required for requests where threed_secure.channel = 02 (Browser).

Field name	Type	Min	Max	Description
browser_color_depth	[0-9]	1	2	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
browser_screen_height	[0-9]	1	6	Total height of the Cardholder's screen in pixels.
browser_screen_width	[0-9]	1	6	Total width of the Cardholder's screen in pixels.
browser_tz	[0-9,-]	1	5	Time difference between UTC time and the Cardholder browser local time, in minutes.
browser_accept_header	[a-zA-Z0-9]	0	2048	Exact content of the HTTP accept headers.
challenge_window_size	[0-5]	2	2	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
user_agent	[a-zA-Z0-9]	5	300	Exact content of the HTTP user-agent header.

Field name	Type	Min	Max	Description
accept_language	[a-zA-Z,]	5	16	Accept-Language header, comma-separated set of locales
version	[a-zA-Z0-9]	1	64	Browser version

Object Name: sdk

Field name	Type	Min	Max	Description
interface	[0-3]	2	2	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
ui_types	Comma separated list	2	14	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
sdk_appid	[0-9azA-Z]	0	36	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

Field name	Type	Min	Max	Description
				must have a canonical form as defined in IETF RFC 4122.
sdk_encdata	[0-9azA-Z]	0	64k	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.
sdk_ephempubkey	[a-zA-Z0-9]	0	255	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
sdk_maxtimeout	[0-9]	2	2	The maximum amount of time (in minutes) for all exchanges. The value must be greater than or equal to 05.
sdk_referencenumber	[a-z0-9]	0	32	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.
sdk_transid	[0-9]	0	36	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.

Object Name: fraud_service

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

Object Name: routing

Field name	Type	Min	Max	Description
request_processor	[a-zA-Z0-9]	0	9	Indicates the selected Processor for the specific transaction. The transaction is routed according to the transmitted value.
requested_processor_mid	[a-zA-Z0-9]	0	32	Indicates the Processor target MID for the specific transaction. The transaction is routed according to the transmitted value
routing_order	[1-9]	1	2	The routing sequence number
method	[a-zA-Z0-9]	1	1	Indicates the Processor Routing Method used for the transaction. Possible values are: 1 – Routing parameter 2 – Routing rules 3 – Processor priority
rule_id	[0-9]	0	4	The Processor Routing Rule ID that was responsible for the routing decision. Only required in cases where method=2.
processor	[A-Z]	0	1,255	The Payment Processor that processed the transaction
target_mid	[a-zA-Z0-9]	0	1,255	The Payment Processor MID
acquirer_transaction_id	[a-zA-Z0-9]	0	1,255	The Payment Processor Transaction ID. Used when corresponding with the Payment Processor or when reconciling transactions.
processor_response	[a-zA-Z0-9]	0	1,255	The original Response Code as transmitted by the Processor
reroute	[a-z]	4	5	Indicates whether Smart Routing reroute is applied to this transaction.
routed_processor	[A-Z]	0	1,255	The first Payment Processor to which the transaction was routed. Only populated in cases where all the following is true: <ul style="list-style-type: none"> Smart Routing is enabled

Field name	Type	Min	Max	Description
				<ul style="list-style-type: none"> The transaction was rerouted to a second processor routing.request_processor was not sent on the request <p>The response did not contain certain result.processor_response_code values</p>
first_processor_response	[a-zA-Z0-9]	0	1,255	<p>The original Response Code as transmitted by the first Payment Processor to which the transaction was routed (i.e., the routing.processor_response of the first Payment Processor to which the transaction was routed). Only populated in cases where all the following is true:</p> <ul style="list-style-type: none"> Smart Routing is enabled The transaction was rerouted to a second processor routing.request_processor was not sent on the request <p>The response did not contain certain result.processor_response_code values.</p>

Object Name: result

Attribute Name	Type	Min	Max	Description
response_code	[0-9]			The Transaction Result Code. For more information, see Appendix B: Operation Result Codes .
response_description	[a-zA-Z0-9]			The transaction result code description. For more information, see Appendix B: Operation Result Codes .

Attribute Name	Type	Min	Max	Description
response_details	[a-zA-Z0-9]			Additional, human readable error description. Providing more details about the error.
original_response_description	[a-zA-Z0-9]			The original Processor Response Message where a rejection does not originate from the <i>Shift4</i> Gateway.
processor_response_code	[0-9]	1	3	Processing Response Reason Code
avs	[A-Z]	1	2	AVS response. The Address Verification Service (AVS) Authorisation response provided by the acquirer at the time of Authorisation.
merchant_advice_code	[0-9]	2	2	Merchant Advice Code (MAC) Indicates whether an attempt to retry the transaction is advised. Possible values: 01: Updated or additional information is needed 02: Try again later 03: Do not try again 04: Token requirements not fulfilled for this token type 21: Payment cancellation
stand_in_service	Object	-		See the stand_in_service object

Object Name: stand_in_service

Returned in response to transactions handled by the stand-in service. If you are not registered to this service you will not receive this object.

Attribute Name	Type	Min	Max	Description
status	[0-9]	1	1	Provides information about a transaction that was handled by the Shift4 stand-in service and the status of the transaction in the stand-in process.

Attribute Name	Type	Min	Max	Description
				<p>Possible values:</p> <ul style="list-style-type: none">1: Transaction pending Credorax stand-in service2: Credorax stand-in service final response3: Transaction does not meet Credorax stand-in max aggregated transaction amount threshold4: Transaction does not meet Credorax stand-in max transaction amount threshold5: Unable to get final answer from the connector / processor. Credorax stand-in service terminated for this transaction

Required Parameters

This chapter describes the required parameters for all payment methods. Specific attributes that are only relevant to specific payment methods are described in [Appendix C - Available Payment Methods](#).

NOTE: In the following tables, **M** indicates a mandatory parameter, **O** indicates an optional parameter, and **C** indicates a parameter that is mandatory in certain cases. Thus, for example, an **M** in the **Sale/Authorisation** column indicates that the parameter is mandatory for Sale and for Authorisation operations.

Root-Level Fields

Parameter Name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
request_id	The merchant's unique Request ID	M	M
payment_method	The selected Payment Method. See the available options in Appendix C - Available Payment Methods	C (Mandatory for Sale/Authorisation only)	-

Object Name: merchant_info

Field Name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
gw_mid	The <i>Shift4</i> -assigned GW MID	M	M
descriptor	The Descriptor displayed to the consumer on the proof of payment	O	-
sub_merchant_id	The Sub-Merchant ID	O	-

Object Name: amount

Field Name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
amount	The requested Billing Amount Two exponents without a decimal are implied apart from currencies with zero exponents. For example, a value of 1000 should	C (Mandatory for Sale/Authorisation; Optional for Payout)	O (Capture, Refund). If missing, the original amount will be considered

Field Name	Description	Sale/Authorisation/ Payout	Capture/Refund/Void/ Re-authorisation
	be transmitted for an amount of 10.00 GBP and a value of 10 should be transmitted for an amount of 10 JPY.		
currency	The Presentment Currency that should be used in the transaction. Any presentment currency you wish to use must be preconfigured on the <i>Shift4</i> platform. Refer to the list of 3 character ISO 4217-alpha-3 currency codes for more information.	C (Mandatory for Sale/Authorisation; Optional for Payout)	O (Capture, Refund). If missing, the original amount will be considered

Object Name: purchase_info

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/ Re-authorisation
free_field	Free Field for the merchant's use	O	-
purchase_order	The Purchase Order number or ID. Identifies this payment.	C (M for MobilePay)	-
description	Description of the purchase	O	-
invoice_number	The purchase's Invoice Number	O	-
mobile_view	Indicates if mobile variant of a scheme is enabled	O	-

Object Name: shipping_address

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/ Re-authorisation
line_1	The shopper's Shipping Address	C (M for PayPal)	-
line_2	The second line of the address. This could be a suite, an apartment number, and so on.	O	-

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
country_code	The Shipping Address Country Code	C (M for PayPal)	-
city	City name	O	-
phone_number	Phone Number	O	-
state	US State Code or the equivalent for other countries. For PayPal transactions only - Required for transactions if the address is in one of the following countries: Argentina, Brazil, Canada, India, Italy, Japan, Mexico, Thailand, or the United States.	O (C for PayPal)	-
postal_code	The Shipping Address' Postal Code	O	-
shipping_method	The Shipping Method used for this purchase	O	-

Object Name: *billing_address*

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
line_1	The shopper's Billing Address	O	-
line_2	The second line of the shopper's address. This can be a suite, an apartment number, and so on.	O	-
country_code	The Billing Address' Country Code	O	-
city	City name.	O	-
phone_number	Phone Number	O	-

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
state	US State Code or the equivalent for other countries. For PayPal transactions only - Required for transactions if the address is in one of the following countries: Argentina, Brazil, Canada, India, Italy, Japan, Mexico, Thailand, or the United States. Maximum length is 40 single-byte characters.	O	-
postal_code	The Billing Address' Postal Code		-

Object Name: *shopper_Info*

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
country_code	The shopper's Country Code	C (Mandatory for Sale/Authorisation; Optional for Payout)	-
birth_date	The shopper's Date of Birth	O	-
last_name	The shopper's Last Name	C (Mandatory for Sale/Authorisation on most payment methods. Optional for Bancontact, SOFORT, EPS, Giropay, iDEAL, P24,) Optional for Payout	-
shopper_id	The specific Payment Method's Shopper ID	O (M for, Trustly, Paysafecard, Entercash, Paysafecash)	-
phone_number	The shopper's personal phone number	C (M for China Union Pay, M for Visa 3DS)	-

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
		Transaction if shopper email is not sent.)	
mobile_phone	The shopper's personal mobile phone number	O	
ip_address	The IP address of the device the shopper is using to initiate the purchase	O	-
first_name	The shopper's First Name	C (Mandatory for Sale/Authorisation on most payment methods. Optional for Bancontact, SOFORT, EPS, Giropay, iDEAL, P24,; Optional for Payout	-
email	The shopper's Email Address	C <ul style="list-style-type: none"> • M for Visa 3DS Transactions. O if phone is sent. • M for Sale/Authorisation with the following payment methods:P24, China Union Pay, Zimpler, Safetypay, Itau, Santander, Webpay, Boletto; • M for Payout 	-
language	The 2-letter Language Code (e.g. de) that should be preferred when presenting payment pages to the consumer	O (Not Relevant for PayPal)	-
iban	Consumer Account IBAN	O	-
bic	Valid BIC (8 or 11 alphanumeric letters)	O (Relevant only for sofort, giropay)	-

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
personal_id	The end-user's Social Security Number/ Personal Identification Number/Birth Number/ etc. Useful for some banks for identifying transactions and for KYC (Know Your Customer)/AML (Anti Money Laundering) purposes.	C (Optional for Trustly;) Mandatory for Bradesco, Bank of Brasil, Itau, Santander, Webpay, Boletto)	-
id_type	Beneficiary's personal identification type.	O	
bank_code	The bank code of the selected bank for the transfer See more details in GET Banks API	O (See more details in GET Banks API)	

Object name: additional_information

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
account_type	The type of account. C: for Current accounts S: for Savings accounts I: International accounts (Relevant only for AstroPay Direct)	M (for AstroPay Direct payouts)	M (for AstroPay Direct refund)
bank_branch	User's bank branch name (Relevant only for AstroPay Direct)	O (for AstroPay Direct payouts)	M (for AstroPay Direct refund)

Object name: redirect_urls

Field name	Description	Sale/Authorisation/Payout	Capture/Refund/Void/Re-authorisation
success_url	The URL to which the user is redirected in the event of a successful transaction	C (Mandatory for Sale/Authorisation Optional for Payout)	-

Field name	Description	Sale/Authorisation/ Payout	Capture/Refund/Void/ Re-authorisation
cancel_url	The URL to which the user is redirected in the event of a cancelled transaction	C (Mandatory for Sale/Authorisation Optional for Payout)	-
fail_url	The URL to which the user is redirected in the event of a failed transaction	C (Mandatory for Sale/Authorisation Optional for Payout)	-
pending_url	The URL to which the user is redirected in the event of a pending transaction	C (Mandatory for Sale/Authorisation Optional for Payout)	-

Object Name: seller_information

This object is required for marketplaces, to provide information about the seller fulfilling the transaction

Field name	Description	Sale/Authorisation/P ayout	Capture/Refund/Void/ Re-authorisation
id	The seller's ID. The ID should be a unique identifier such as the seller name or an internal registration number. This field is mandatory sending this the seller_information object.	C (Sale only)	C (Capture only)
country	The seller's country.	C (Sale only)	C (Capture only)
city	The seller's city.	C (Sale only)	C (Capture only)
line_1	The seller's address.	C (Sale only)	C (Capture only)
postal_code	The seller's postal code.	C (Sale only)	C (Capture only)
state	The seller's state.	C (Sale only)	C (Capture only)

Object Name: threed_secure

Field name	Description	Sale/Authorisation/P ayout	Capture/Refund/Void/ Re-authorisation
cavv	The authentication value received from the issuer	O	-
eci	The ECI assigned to the authentication	O	-
xid	XID generated as part of the authentication. Relevant only for 3D Secure version 1.0.2	O	-
version	Indicates the 3D Secure protocol version Possible values: <ul style="list-style-type: none"> 1.0 2.0 2.1.0 2.2.0 	C (M if using cavv/eci/xid)	-
dstrxid	3DS Directory server transaction ID. Must be sent if threed_secure.version = 2.0 or higher, and threed_secure.eci, threed_secure.cavv are used. Refer to Appendix E: How to provide 3D secure Authentication Data	C (M if threed_secure.version = 2.0 or higher)	-
initiate	Indicates whether to initiate the Shift4 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 (see 3DS Adviser) For additional information about the 3D Secure process, see Payments API Appendix D: SCA & 3D Secure . Note: If the transaction contains all the following parameters, it will be declined:	O (default value: 02)	-

Field name	Description	Sale/Authorisation/P ayout	Capture/Refund/Void/ Re-authorisation
	threeed_secure.initiate, threeed_secure.eci, and threeed_secure.cavv		

Object name: payment_details

Field name	Description	Sale/Authorisation/P ayout	Capture/Refund/Void/ Re-authorisation
recurring	Indicates whether the transaction is the first of a recurring series of payments or a subsequent payment in the series. Possible values: <ul style="list-style-type: none"> FIRST SUBSEQUENT 	0	-
partial_capture_indicator	Partial capture indicator Accepted values: <ul style="list-style-type: none"> true false To be used with Israeli processors only.	0	-
cardholder_name	Cardholder full name	C (m for 3D secure transaction)	-

Response Message Format

Shift4 reserves the right to return an echo of the request parameters as well as additional response parameters at any time.

NOTE: In the following tables, **M** indicates a parameter that must be returned, **O** indicates a parameter that could optionally be returned, and **C** indicates a parameter that must be returned in certain cases.

Attribute Name	Type	M/O/C	Description
payment_id	[a-zA-Z0-9]	M	The <i>Shift4</i> -generated Payment ID. Payment_id aggregates several transaction_ids.
transaction_id	[a-zA-Z0-9]	M	The <i>Shift4</i> -generated Transaction ID. Each request to results in a unique transaction_id.
request_id	[a-zA-Z0-9]	M	An echo of the unique transaction_id that the merchant had transmitted to <i>Shift4</i> when creating the payment request.
pr_transaction_id	[a-zA-Z0-9]	C	Payment Processor Transaction ID. The unique transaction_id created by the Payment Processor.
payment_method	[a-zA-Z]	M	The selected Payment Method.
operation	[a-zA-Z]	M	One of the following: Sale, Authorisation, Capture, Void, Refund, Re-Authorisation
transaction_time	string	M	Time of the Transaction in UTC format dd-MM-yy HH:mm:ss:SSS

Object Name: *purchase_info*

Attribute Name	Type	M/O/C	Description
invoice_number	[a-zA-Z0-9]	O	The Invoice Number used for tracking this payment
free_field	[a-zA-Z0-9]	O	Free Field for the shopper's use
purchase_order	[a-zA-Z0-9]	C	The Purchase Order number or ID. Identifies this payment. Note: <ul style="list-style-type: none"> Optional for most payment methods Mandatory for MobilePay
description	[a-zA-Z0-9]	O	Description of the purchase
payment_type		O	Indicates the payment type that was used 00 - Bank Transfer Online (EFT) 01 - Bank Transfer Offline 02 - Boletto / Invoice

Attribute Name	Type	M/O/C	Description
			03 - Debit or Credit Card (Relevant only for AstroPay Direct)
funding	true false	O	This field has a value of "true" if the transaction is AFT. Otherwise, the field does not appear in the response.

Object Name: shopper_info

Attribute Name	Type	M/O/C	Description
shopper_id	[a-zA-Z0-9]	O	The relevant APM Shopper ID if applicable. This holds the payer_id in the case of PayPal transactions.
account_holder	[a-zA-Z0-9]	O	The Consumer Account's Account Holder
iban	[0-9]	O	Consumer Account IBAN
bic	[0-9]	O	Consumer Account BIC
bank_name	[a-zA-Z0-9]	O	Consumer Account Bank Name
bank_code	[A-Za-z]	O	The bank code of the selected bank for the transfer See more details in the GET Banks API

Object Name: result

Attribute Name	Type	M/O/C	Description
response_code	[0-9]	M	The Transaction Result Code. For more information, see Appendix B: Operation Result Codes .
response_description	[a-zA-Z0-9]	M	The transaction result code description. For more information, see Appendix B: Operation Result Codes .
response_details	[a-zA-Z0-9]	O	Additional, human readable error description. Providing more details about the error.
original_response_description	[a-zA-Z0-9]	O	The original Processor Response Message where a rejection does not originate from the <i>Shift4 Payments Platform</i> .
processor_response_code	[0-9]	m	Processing Response Reason Code
avs	[A-Z]	o	AVS response. The Address Verification Service (AVS) Authorisation response provided by the acquirer at the time of Authorisation.
merchant_advice_code	[0-9]	o	Merchant Advice Code (MAC)

Attribute Name	Type	M/O/C	Description
			Indicates whether an attempt to retry the transaction is advised. Possible values: 01: Updated or additional information is needed 02: Try again later 03: Do not try again 04: Token requirements not fulfilled for this token type 21: Payment cancelation
stand_in_service	Object	-	See the stand_in_service object

Object Name: stand_in_service

Attribute Name	Type	M/O/C	Description
status	[0-9]	0	Indicates whether the transaction was handled by the Shift4 stand-in service as well as the transaction status. Possible values are: 1: Transaction pending Credorax stand-in service 2: Credorax stand-in service final response 3: Transaction does not meet Credorax stand-in max aggregated transaction amount threshold 4: Transaction does not meet Credorax stand-in max transaction amount threshold 5: Unable to get final answer from the connector / processor. Credorax stand-in service terminated for this transaction

Object Name: amount

Attribute Name	Type	M/O/C	Description
amount	[0-9]	0	The requested Billing Amount Two exponents without a decimal are implied apart from currencies with zero exponents. For example, a value of 1000 should be transmitted for an amount of 10.00 GBP, but a value of 10 should be sent for an amount of 10 JPY.

Attribute Name	Type	M/O/C	Description
currency	3 character ISO 4217-alpha-3 currency code	O	The Presentment Currency that should be used in the transaction. Any Presentment Currency you wish to use must be preconfigured on the Shift4 Payments platform.

Object Name: links

Attribute name	Type	M/O/C	Description
href method re	string	O	Object containing links to operations related to the executed operation.

Object Name: additional_information

This object includes fields used by certain payment methods.

Field name	Type	M/O/C	Description
multibanco_reference	[a-zA-Z0-9]	O	The payment reference of the transaction. Relevant only for multibanco.
Multibanco_entity	[a-zA-Z0-9]	O	The entity reference of the transaction. Relevant only for multibanco.
P24_descriptor	[a-zA-Z0-9]	O	Przelewy24 doesn't allow setting a client specific payment descriptor, instead a payment identifier is generated. To allow supporting consumers this payment descriptor is returned in the specific output parameter.

Object name: redirect_urls

Field name	Type	M/O/C	Description
redirect_url	URL	C	Received in the response message and indicates to which URL to redirect the shopper. Contains one of the following values: <ul style="list-style-type: none"> From a payment method: The URL to which the user is redirected in order to complete the purchase From the issuer (for 3D Secure): The issuer's URL for the 3D secure authentication process

Field name	Type	M/O/C	Description
redirect_url_app	URL	C (M for MobilePay)	Received in the response message and indicates to which mobile application URL to redirect the shopper.

Object name: payment_details

Field name	Type	M/O/C	Description
authorization_code	[a-zA-Z0-9]	O	Authorisation Code
rrn	[0-9]	O	The transaction's Retrieval Reference Number (RRN). The RRN may be provided by the processor as an additional identifier of the transaction. Every refund transaction will receive a unique RRN, different from the initial transaction RRN.
initial_transaction_id	[a-zA-Z0-9]	O	Initial transaction ID. Received as part of the initial transaction response parameters. Must be sent for every subsequent 'merchant initiated transaction'.
fast_funds_indicator	[A-Z]	O	Fast funds indicator. Indicates whether the issuer supports fast funds functionality. Possible values are: Y – Supports fast funds for domestic & cross-border payments C – Supports fast funds for cross-border payments

Field name	Type	M/O/C	Description
			D – Supports fast funds for domestic payments N – No result
token	JSON	O	Used for the following: <ul style="list-style-type: none"> The token created if the create_token parameter was used The assigned payment token for mobile payments. See token in Additional request parameters for Apple Pay & Google Pay
payment_account_reference	[a-zA-Z0-9]	O	PAR - Payment Account Reference

Object name: *payment_details.fraud*

Field name	Type	M/O/C	Description
score	[0-9]	O	Risk Score. The fraud-protection service's response. The transaction will be rejected if the risk score is greater than or equal to the threshold defined in the merchant setup, but will continue being processed if its risk score is lower than the merchant-defined threshold.
sent_to	[A-Z]	O	Indicates the result of the transaction's transmission to the fraud-protection service.
explanation_array	[a-zA-Z0-9]	O	Fraud Explanation Array. Indicates the risk score and provides the list of rules that were triggered by the transaction in question.

Object name: *routing*

Field name	Type	M/O/C	Description
method	[a-zA-Z0-9]	O	Indicates the Processor Routing Method used for the transaction. Possible values are: 1 – Routing parameter

Field name	Type	M/O/C	Description
			2 – Routing rules 3 – Processor priority
rule_id	[0-9]	O	The Processor Routing Rule ID that was responsible for the routing decision. Only populated in cases where method=2.
processor	[A-Z]	O	The Payment Processor that processed the transaction
target_mid	[a-zA-Z0-9]	O	The Payment Processor MID
acquirer_transaction_id	[a-zA-Z0-9]	O	The Payment Processor Transaction ID. Used when corresponding with the Payment Processor or when reconciling transactions.
processor_response	[a-zA-Z0-9]	O	The original Response Code as transmitted by the Processor
reroute	[a-z]	O	Indicates whether Smart Routing reroute is applied to this transaction.
routed_processor	[A-Z]	O	The first Payment Processor to which the transaction was routed. Only populated in cases where all the following is true: <ul style="list-style-type: none"> • Smart Routing is enabled • The transaction was rerouted to a second processor • routing.request_processor was not sent on the request • The response did not contain certain result.processor_response_code values
first_processor_response	[a-zA-Z0-9]		The original Response Code as transmitted by the first Payment Processor to which the transaction was routed (i.e., the routing.processor_response of the first Payment Processor to which the transaction was routed). Only populated in cases where all the following is true: <ul style="list-style-type: none"> • Smart Routing is enabled • The transaction was rerouted to a second processor • routing.request_processor was not sent on the request • The response did not contain certain result.processor_response_code values.

Object Name: threed_secure

Field name	Type	M/O/C	Description
eci	[0-9]	O	The ECI assigned to the authentication
cavv	[a-zA-Z0-9]	O	The authentication value received from the issuer
xid	[a-zA-Z0-9]	O	XID generated as part of the authentication. Relevant only for 3D Secure version 1.0.2
trxid	[a-zA-Z0-9]	O	The assigned 3D transaction ID
threds_status	[A-Z]	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 C – Challenge Required; Additional authentication is required 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
valid_payment	[yn]	O	Shift4 recommendation whether to initiate payment following the authentication results. Possible values: y – yes n – no
version	[0-9]	O	Indicates the 3D Secure protocol version Possible values: <ul style="list-style-type: none"> 1.0 2.0 2.1.0 2.2.0
pareq	[a-zA-Z0-9]	O	Relevant only for 3D secure 1.0 flows. Used when accessing the URL provided in redirect_urls.redirect_url

Field name	Type	M/O/C	Description
acstansid	[a-zA-Z0-9\-.]	O	Unique transaction identifier assigned by the ACS to identify a single 3D secure transaction.

Retrieval (GET) Transaction Format Purpose

The purpose of a GET transaction is to query the result of a certain transaction.

It is not recommended to create a GET transaction link on your own, but rather employ the returned links to this end. The following table describes the GET links' logic.

Link Format

GET URLs:

Operation	URL
GET Authorisation Info	https://sourcepayments.com/payments/rest/authorize/gw_mid/sub_merchant_id/transaction_id
GET Sale Info	https:// sourcepayments.com/payments/rest/sale/gw_mid/sub_merchant_id/transaction_id
GET Capture Info	https:// sourcepayments.com/payments/rest/capture/gw_mid/sub_merchant_id/transaction_id
GET Void Info	https:// sourcepayments.com/payments/rest/void/gw_mid/sub_merchant_id/transaction_id
GET Refund Info	https:// sourcepayments.com/payments/rest/refund/gw_mid/sub_merchant_id/transaction_id

Note: The sub_merchant_id field is relevant only for PF transactions.

Request Format

The GET request should be as described in the GET URLs table. There is no "Body" to the transaction retrieval request. Furthermore, the request headers are identical to the original request's headers.

Example

Headers:

Authentication: Bearer

3ebbc329f44b96abb20a560529e6df962dc67722bc5503d25ee561a4b83931330b8e5b98c8d23d711ed6f172e256459e468bafeb85256081561a6690ac5e859d

URL:

https:// sourcepayments.com/payments/rest/void/gw_mid//trx_id_123456

Response Format

Identical to the original transaction response described in [Response Message Format](#).

Timeout Handling

If a transaction takes too long to return a response, a timeout is initiated by the Gateway application and result code “007” is returned. Nonetheless, a transaction may eventually be successfully processed by the payment processor, even though the gateway already returned a timeout response. In order to be informed of such cases, it is highly recommended to initiate a GET request after a transaction processing request if no [Notifications](#) are enabled.

GET Banks API

When you initiate a Sale transaction with a payment method which requires to specify the bank code (bank_code), use the following 'GET Banks' API call to retrieve a list of the available banks in a specified country. You can then display the list of available banks to your shopper, based on the response of the API.

API name: get_banks

Request Method: POST

Request parameters

Parameter name	Type	M/O/C	Description
gw_mid	[0-9A-Za-z]	M	The <i>Shift4</i> -assigned gateway MID (Merchant ID)
payment_method	[0-9A-Za-z]	M	The selected Payment Method. See the available options in Appendix C - Available Payment Methods
request_id	[0-9A-Za-z]	M	Merchant-generated unique Request ID

Object name: shopper_info

Parameter name	Type	M/O/C	Description
country_code	[A-Z]	M	The shopper's 2-letter ISO Country Code. Refer to ISO 3166-1-alpha-2 for a list.

Response Format

The response is JSON formatted, and can include more than a single object. Each object is constructed from the following parameters:

Parameter name	Description
code	Bank code
name	Bank name
logo	URL pointing at bank's logo
Payment_type	bank's payment type code

Example:

```
{
  "payment_id": "CPP-4ossss9dodd29495656593s20DZA",
  "transaction_id": "TCP-ossss9dodd29495656593s20JKTP",
```

```
"request_id": "4ossss9dodd95656593s20",
"transaction_time": "15-07-19 07:42:20:293",
"payment_method": "astropay",
"operation": "GET_BANKS",
"result": {
  "response_code": "000",
  "response_description": "Request processed successfully."
},
"shopper_info": {
  "country_code": "AR"
},
"merchant_info": {
  "gw_mid": "10000510"
},
"allowed_banks": [
  {
    "name": "Itau",
    "code": "I",
    "logo":
"https://sandbox.astropaycard.com/images/logo_itau.jpg",
    "payment_type": "00"
  },
  {
    "name": "Dinero Mail - Transferencia",
    "code": "DD",
    "logo":
"https://sandbox.astropaycard.com/images/DMlogo.jpeg",
    "payment_type": "00"
  },
]
}
```

PayPal Specifications

This chapter is relevant only to PayPal transactions.

Web Experience Profile ID

The PayPal onboarding process requires you to define your own Web Experience Profile ID and register it during the onboarding process. The Web Experience Profile ID allows you to customise your PayPal page according to your preferences and offer your shoppers a seamless Checkout experience. In order to apply it, you need to send your Web Experience_Profile_ID when transmitting a PayPal Sale and Authorisation transaction.

You can define the following parameters of your Web Experience_Profile_ID during your *Shift4* onboarding process:

1. Present the shopper with either the Continue or Pay Now checkout flows.
2. The display of the Shipping Address
3. The source of the Shipping Address
4. A Brand Name (overrides the Business Name in the PayPal account)
5. Adding your logo to the PayPal checkout page
6. Choosing the language displayed on your PayPal checkout page.

Field Name	Type	Min	Max	M/O	Description
experience_profile_id	string	2	128	0	The merchant's registered PayPal Web Experience ID. The merchant determines the experience profile and then registers it as part of the PayPal onboarding process.

Special Processing Requirements

The following are additional parameters that are unique to PayPal transactions:

Field Name	Type	Min	Max	M/O	Description
final_capture	boolean	1	1	0	Indicates whether or not the Capture is final. Mostly relevant to cases in which the captured amount is lower than the authorisation amount and no further Captures are expected.

Object Name: merchant_info

Field Name	Type	Min	Max	M/O	Description
order_url	URL	32	2048	O	The Merchant Site URL related to this payment
message_to_payer	[a-zA-Z0-9]	0	165	O	A Free-Form field that the merchant can use for sending a note to the shopper

Object Name: purchase_info

Field Name	Type	Min	Max	M/O	Description
payment_options	string	0	21	O	One of the following: <ul style="list-style-type: none"> UNRESTRICTED: The merchant does not have a preference for a shopper Payment Method. This is the default value. INSTANT_FUNDING_SOURCE: The merchant requires that the shopper pay using an Instant Funding source, such as a credit card or PayPal balance. All payments are processed instantly. However, payments that require manual review are marked as pending. Merchants must handle the pending state as an incomplete payment. IMMEDIATE_PAY: Process all payments immediately. Any payment that requires manual review is marked as failed.
Items [quantity, price, name, description, currency, url]	array	1	256	M	An array containing information about the purchased item(s), which is made up of objects containing the detailed fields. Several items mean that the array contains several objects.
digital_goods	boolean	1	1	O	Indication of whether digital goods were purchased.
one_click	boolean	1	1	O	Indicates whether the transaction is of the “1-click” type. Relevant to the Express Checkout Shortcut flow.
user action	String	6	8	O	Defines whether the shopper is to be presented with a Continue or Pay Now checkout flow. For the Pay Now checkout flow, set user_action=commit For the Continue checkout flow, set user_action=continue (default)

Object Name: amount.amount_details

Field Name	Type	Min	Max	M/O	Description
subtotal	string	1	10	O	Item Subtotal amount
shipping	string	1	6	O	Shipping Fee
tax	string	1	6	O	Tax portion of the price
handling_fee	string	1	6	O	Purchase Handling Fee
discount	string	1	6	O	Shipping Fee Discount
insurance	string	1	6	O	Insurance Fee
gift_wrap	string	1	6	O	Gift Wrap Fee

PayPal Seller Protection Program (SPP)

The [PayPal Seller Protection Program](#) is a fraud-protection service that helps you to monitor fraud activity and reduce chargebacks. If you wish to use the SPP service, send the following fields as part of the Sale, Authorisation and Use Token requests.

Note that you need to contact PayPal in advance and request to enrol in the program in order to benefit from this service.

Object Name: OTA (Online Travel Agency)

Field Name	Type	Min	Max	Description
Type	string	3	32	OTA (Online Travel Agency) type: hotel/train ticket/ferry/bus/multi-modal
service_start_date	ISO 8601 date format	1	32	OTA Service Start Date. A Service Start Date that is very close to the Transaction Date indicates an elevated level of risk.
service_end_date	ISO 8601 date format	1	32	OTA Service End Date. A consumer booking a service such as a hotel for an abnormally long period of time indicates an elevated level of risk.
changable	boolean	1	1	Whether or not the guest (the person being served) can be changed. Fraudsters tend to pay for services where the guest can be changed.
start_country	ISO Alpha-2 Country Code	2	2	OTA Start Country such as the hotel's country. PayPal compares this variable to the transmitter's Country / IP Country / Billing Country for risk management purposes.

Field Name	Type	Min	Max	Description
end_country	ISO Alpha-2 Country Code	2	2	OTA End Country
start_city	string	2	64	Initial Service City
end_city	string	2	64	Final Service City
start_zipcode	string	3	12	Initial Service ZIP Code
end_zipcode	string	3	12	Final Service ZIP Code
start_adress_line1	string	2	64	Address (Line 1) of initial service location
end_adress_line1	string	2	64	Address (Line 1) of final service location

Object Name: STC (Set Transaction Context)

Field Name	Type	Min	Max	Description
first_date	string	1	32	Date of the first interaction between the sender and receiver on the Partner/Merchant platform. An interaction can be defined as IM, Call, Money Transfer, Add as Friend, etc., depending on the partner.
txn_count_3_month	string	1	10	Number of transactions the shopper has completed on the Partner/Merchant platform (through PayPal or otherwise) in the last three months
txn_count_total	string	1	12	Total number of transactions the shopper has completed on the Partner/Merchant platform (through PayPal or otherwise) thus far
txn_count_24_hr	string	1	5	Number of transactions the shopper has completed on the Partner/Merchant platform (through PayPal or otherwise) in the past 24 hours
txn_count_1_hr	string	1	4	Number of transactions the shopper has completed on the Partner/Merchant platform (through PayPal or otherwise) in the past hour
transaction_is_tangible	boolean	1	1	The Merchant's transaction is for tangible rather than digital goods. An event ticket is only considered a tangible good only if it produces some proof of shipping such as a Tracking Number or Shipping Address. It is considered intangible in all other cases (e.g. email, pickup at venue).

Field Name	Type	Min	Max	Description
loyalty_flag_exists	boolean	1	1	Whether or not a Merchant Loyalty Flag is present
highrisk_txn_flag	boolean	1	1	Whether or not the transaction is for high-risk items such as Gift Cards or any cash equivalent
vertical	string	1	32	Transaction-level Vertical Identifier for Partner/Merchant transactions that are in several verticals such as “retail”
delivery_method	email, phone, venue_ pickup, kiosk_pi ckup	1	32	Delivery Method for an intangible item if there is an associated email/phone number. This serves as the Shipping Address for an intangible item.

The following tables list the OTA and STC data fields required for particular industries or verticals. Merchants who belong to these particular industries or verticals must transmit those data fields in the OTA or STC payload respectively.

Field Name	Retail/Food	OTA–Transportation / Car Rental	OTA-Travel package	Event and Ticketing
type	-	M	M	-
service_start_date	-	M	M	-
service_end_date	-	M	M	-
changable	-	M	M	-
start_country	-	M	M	-
end_country	-	M	-	-
start_city	-	M	-	-
end_city	-	M	-	-
start_zipcode	-	M	-	-
end_zipcode	-	M	-	-
start_adress_line1	-	M	-	-
end_adress_line1	-	M	-	-

Field Name	Retail/Food	OTA-Transportation / Car Rental	OTA-Travel package	Event and Ticketing
first_date	-	M	M	M
txn_count_3_month	M	M (transportation only)	-	M
txn_count_total	-	M (transportation only)	-	M
txn_count_24_hr	-	-	-	M
txn_count_1_hr	-	-	-	M
transaction_is_tangible	-	-	-	M
loyalty_flag_exists	M	M (transportation only)	-	M
highrisk_txn_flag	M	-	-	-
vertical	M	-	-	-
delivery_method	M	-	-	M

Fraudnet/Magnes SDK Information

PayPal requires the execution of Fraudnet or Magnes as part of the RDA (Risk Data Acquisition). This is the protection suite PayPal offers to merchants. More specifically, RDA improves fraud handling with dynamic data management and provides real-time controls for all merchant categories. In addition, RDA Improves PayPal merchants and partners' Seller Protection.

Fraudnet

Needed for every Authorisation, Sale (with and without a Token) and Create Token scenario involving the presence of a shopper.

Magnes

Needed for every Authorisation, Sale (with and without a Token) and Create Token scenario involving the presence of a shopper and the initiation of a transaction from a native mobile application.

Specific Processing Rules & Disclaimers

1. PayPal displays a **Continue** button on its hosted pages by default. If there are no additional steps after the PayPal-hosted pages, the **Pay Now** button should be displayed on the last PayPal-hosted page.
2. When the Express Checkout Shortcut is applied:
 - a. The shopper is not to be required to log into their account

- b. No shipping address is requested to be displayed on the merchant's
3. Express Checkout Shortcut (Traditional PayPal Flow):
 - a. The official *Checkout with PayPal* button must be located on the product page.
 - b. The official *Checkout with PayPal* button must be located on the shopping cart page.
 - c. The shopper can complete the purchase in two or fewer steps after being redirected from PayPal to the merchant's website.
4. Refunds can be performed by the merchant within 180 days of the day of payment.
5. Only full refunds are possible for disputed transactions. Attempting to transmit a partial refund will return an error from the PayPal side.

Branding

1. The PayPal acceptance mark should be displayed alongside all other payment acceptance or payment services marks on your website. You can find the PayPal acceptance mark here: <https://www.paypal.com/brandassets>.
2. You can configure your PayPal account to display your logo on the checkout page in the following URL: https://www.paypal.com/webscr?cmd=_profile-page-styles&CALL_FORM_UPDATE=false
3. The PayPal pages may be localised in any PayPal-supported language. See the following URL for details: <https://developer.paypal.com/docs/integration/direct/rest/locale-codes/>. You can set the locale as part of your Web Experience Setup.
4. The PayPal FAQ popup should be displayed when a shopper clicks on the [PayPal mark](#).
5. Always use the correct capitalisation of PayPal in text and images (and not "Paypal", "paypal", "Pay Pal", etc.)
6. Payment page best practices:
 - d. Card payment fields are to be disabled or hidden upon the selection of PayPal as a payment option.
 - e. No payment method is to be pre-selected by default
 - f. The PayPal logo is to be displayed alongside and in the same size and manner as other payment methods

Apple Pay Specifications

Apple Pay is Apple's alternative payment method allowing Apple users to pay with their devices.

How does it work?

Apple Pay uses device-specific tokenised credit or debit card credentials (DPAN) in place of a Payment Account Number (PAN). When a customer confirms the payment using Face ID, Touch ID or passcode, the tokenised card data is returned to your app or website. This token can then be passed on to your Payment Service Provider (PSP) to process as you would a typical online credit or debit card payment.

Any transaction type you support today for regular debit and credit cards can be performed with Apple Pay, including refunds. Apple Pay works on Apple devices running iOS, watchOS and iPadOS both in-app and in Safari, and on macOS devices in Safari.

Apple Pay integration

You can integrate with Apple Pay either from in-app or from the web transaction. You need to implement Apple APIs to verify that Apple Pay can be offered as a payment method:

- Integrate with the PassKit SDK to offer Apple Pay from in-app, as described in [PassKit](#).
- Integrate with Apple Pay JS to offer Apple Pay from a web transaction, as described in [Apple pay js](#).

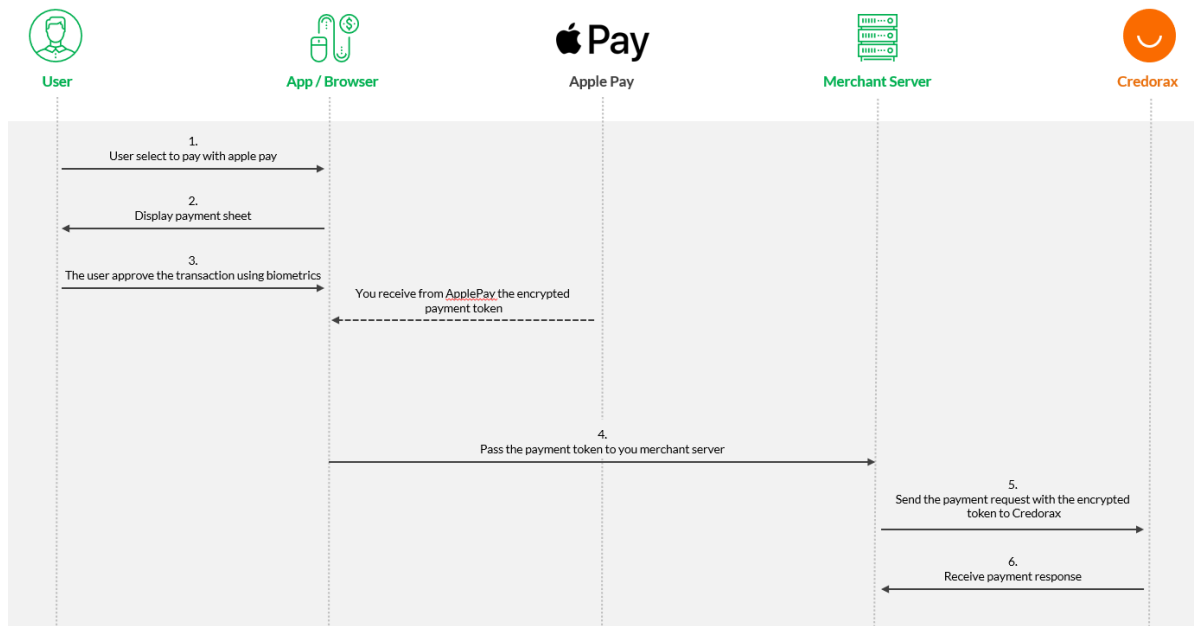
After integrating with Apple Pay, you will be able to request an encrypted payload from Apple. Apple in turn will create a "payment token" that includes an encrypted "payment data" object. You should pass this "payment data" object to the Shift4 gateway in the "token" field (described in [token](#)) for decryption and processing.

Registration with Apple

Before starting, you need to make sure you complete the following steps on your Apple account:

1. Register for an Apple developer account. You need to enroll as an Apple Pay developer, and go through the Apple certification process as described [here](#).
2. If you are integrating Apple Pay on the web (using Safari) make sure your server supports Apple's additional security requirements described [here](#).
3. Get a CSR file from Shift4.
4. Upload the signed CSR to Shift4.
5. Add an Apple Pay button to your app or website. Use the appropriate PassKit or JavaScript APIs to render the button in your app or website so the button will always be up-to-date and localised. More details can be found in: <https://developer.apple.com/design/human-interface-guidelines/apple-pay/overview/introduction/>.

Transaction flow



1. You (the merchant) offer Apple Pay as a payment method.
2. The shopper selects to pay with Apple Pay.
3. You trigger a call to Apple.
4. The payment sheet is displayed to the shopper. The merchant is responsible for the information that is displayed on the Apple payment sheet.
5. After shopper authentication via Face ID, Touch ID or passcode, your app or website receives the PKPayment or ApplePayPayment object.
6. You pass the token information from your client side to your server side.
7. You pass the payment token to Shift4 in the “token” field alongside other payment information.
8. Shift4 verifies the authenticity of the token, decrypts its values, and sends to the relevant processor.
9. After receiving a response from your payment service provider, you return a Success or Fail response to the Apple Pay API to inform the shopper and dismiss the payment sheet. After the payment sheet is dismissed, you display your general transaction confirmation screen.



Note:

In addition to the standard request parameters, Apple Pay may require additional parameters listed in the chapter

Google Pay Specifications

Google Pay is a payment method allowing Google users to pay with their devices.

How does it work?

Google Pay uses both device-specific tokenised credit or debit card credentials (DPAN) in place of a Payment Account Number (PAN) and PAN. When a customer confirms the payment using Face ID, Touch ID or passcode, the tokenised card data is returned to your app or website. This token can then be passed on to the Shift4 gateway to process as you would a typical online credit or debit card payment.

Any transaction type you support today for regular debit and credit cards can be performed with Google Pay, including refunds. Google Pay works on all major web and mobile web browsers.

Google Pay integration

You can integrate with Google Pay either from in-app or from the web transaction. You need to implement Google APIs in order to initiate the Google Pay transaction.

After integrating with Google Pay, you will be able to request an encrypted payload from Google. Google in turn will create a “payment token” that includes an encrypted “payment data” object. You should pass this object to the Shift4 gateway in the “token” field (described in [token](#)) for decryption and processing.

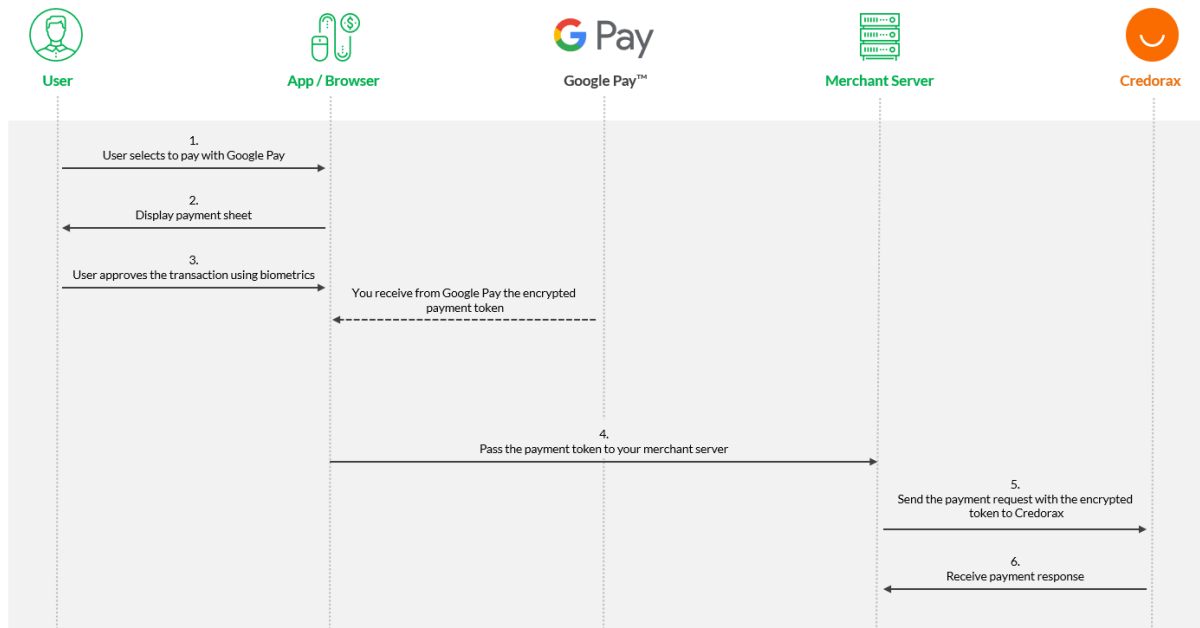
Android Integrations

See more details on [Google Pay Android developer documentation](#), [Google Pay Android integration checklist](#) and [Google Pay Android brand guidelines](#).

Web Integrations

See more details on [Google Pay Web developer documentation](#), [Google Pay Web integration checklist](#) and [Google Pay Web Brand Guidelines](#).

Transaction flow



1. You (the merchant) offer Google Pay as a payment method.
2. The shopper selects to pay with Google Pay.
3. You trigger a call to Google from the device/web, specifying:
 - g. Gateway: credorax
 - h. gatewayMerchantID: refer to [gw_mid](#)
4. The payment sheet is displayed to the shopper.
5. After shopper authentication, your app or website receives the payment data object encrypted with the Shift4 unique key.
6. You pass the token information from your client side to your server side.
7. You pass the payment token to Shift4 in the “token” field alongside other payment information.
8. Shift4 verifies the authenticity of the token, decrypts its values, and sends to the relevant processor.
9. After receiving a response from Shift4, you display the confirmation page to the shopper.

MobilePay Specifications

MobilePay is a local payment method popular in Nordics countries, mostly in Denmark but also in Finland and Greenland. It allows its users to store a payment card on the digital wallet and pay with it online.

Supported Shopper Countries	Denmark, Finland, Greenland
Supported Operations	<ul style="list-style-type: none">• Sale• Authorization• Capture• Void• Refund• Payout
MobilePay features currently not supported	Checkout
Browsers	Supported by all major web and mobile web browsers

How to prepare for processing MobilePay

Before you begin processing MobilePay you have to complete the following steps:

1. Request to add MobilePay to your Shift4 account. See details in Appendix F: Setting up with MobilePay
2. Add the MobilePay button to your checkout page. Refer [to MobilePay's website for guidelines](#)

Sale Transaction Flow

1. Offer MobilePay as a payment method in your checkout flow
2. The shopper selects to pay with MobilePay.
3. You trigger a Sale API call to Shift4 with all the details required in this document. Refer to chapters: [General message format](#); [Description of objects and fields](#); [Required parameters](#)
4. The response to this call contains a redirect URL that you should present to the shopper
5. The shopper identifies with mobilepay through the URL
6. The transaction is processed, and the shopper is redirected by mobilepay to the success/fail URL you defined according to the transaction result.
7. You receive a transaction response with indication on the result of the transaction.

Note:

- Make sure you send the `purchase_info.purchase_order` parameter with every transaction
 - As part of MobilePay's retry flow which allows the cardholder to retry the payment with another card through MobilePayu app, additional payment attempts can be initiated, and this value can be used as the identifier to all payment attempts.
- For using the MobilePay's future pre-filled phone number, make sure you send the `shopper_info.phone_number` on the transaction.
- For redirecting the cardholder directly to MobilePay's application instead of MobilePay's website, use the `redirect_url_app` that is returned on the response. Make sure you use this URL only when the cardholder is in a mobile app.
- Payments with MobilePay require SCA (where applicable). MobilePay attempts to authenticate the shopper with their own SCA solution, but sometimes the transaction may require 3D Secure. To ensure a smooth processing experience, we recommend to include 3D Secure parameters with every transaction. To do that, you have to be registered to Shift4 3D Secure service. Refer to [Appendix D: SCA & 3D Secure](#) for more details
- Redirecting the user to the return page should solely rely on data given in the redirect
- Processing the purchase should rely on the response received you PSP, and not on the interaction with the customer



Payout

Payout is the process of paying funds to the shopper's account. You can process a referral payout against a previous original MobilePay transaction.

Note:

Payouts in MobilePay are not reflected on the shopper's MobilePay app. Since MobilePay is a wallet, the funds are transferred directly to the shopper's card which is connected to their MobilePay account.



Additional Request Parameters for Specific Payment Methods

Some payment methods require additional parameters to be included when processing transactions. This section provides information about them. The below fields are applicable for Apple Pay, Google Pay and MobilePay

Object Name: *payment_details*

Field Name	Type	Min	Max	M/O/C	Description
token	^.+\$	0	4096	M	The assigned payment token. The payment token can be assigned by Shift4 or by the mobile digital payment platform such as Google Pay or Apple Pay.
pan	[0-9]	8	19	C (M for Independent Payout)	PAN – Primary Account Number
expiry_month	[0-9]	2	2	C (M for Independent Payout)	Card expiration month in two-digit format (mm)
expiry_year	[0-9]	2	2	C (M for Independent Payout)	Card expiration year in two-digit format (yy)
source_type	[A_Z]	4	9	M	Possible values: <ul style="list-style-type: none"> • ECOMMERCE • PHONE • MAIL • VPOS

Field Name	Type	Min	Max	M/O/C	Description
recurring	[A_Z]	5	10	O	Indicates whether the transaction is the first of a recurring series of payments or a subsequent payment in the series. Possible values: <ul style="list-style-type: none"> FIRST SUBSEQUENT
card_on_file	[A_Z]	4	9	O	Indicates whether the transaction is Merchant Initiated or Cardholder Initiated. This parameter is not required when a recurring transaction is sent. Possible values: <ul style="list-style-type: none"> MIT CIT
card_validation	[A_Z]	4	5	O	Indicates whether the transaction is for card validation purposes. This parameter is not required if a recurring or card_on_file transaction is sent. By default the parameter's value is False. Possible values: <ul style="list-style-type: none"> TRUE FALSE
authorization_type	[A_Z]	3	5	O	Authorisation Type. Possible values: <ul style="list-style-type: none"> FINAL PRE Note that transactions referring to Pre-Authorisations must be sent with amount details.
expected_captures	[0-9]	1	2	O	Indicates the number of expected Captures. This parameter is only supported in Card-not-Present transactions. The default value is 1. The maximum value is 98. The minimum merchant-settable value is 2.
skip_card_validation	[A_Z]	4	5	O	Relevant only when creating a token . This parameter can be used in cases where you wish to create the token on the Shift4 systems without pre-validating the card. This functionality requires obtaining Shift4 permission and performing some setup operations.

Field Name	Type	Min	Max	M/O/C	Description
card_type	[A_Z]	3	10	O	Card Brand. Possible values are: <ul style="list-style-type: none"> VISA MASTERCARD AMEX ISRACARD MAESTRO JCB DISCOVER DINERS
initial_transaction_id	[0-9]	13	13	C	Initial transaction ID. The same value received as part of the original transaction response parameters. This must be sent to ensure the transaction is considered a Merchant Initiated Transaction (MIT).

Object Name: recipient_info

Field Name	Type	Min	Max	M/O/C	Description
first_name	[a-zA-Z0-9]	3	32	C (M for CFT/ AFT)	The recipient's First Name. If shorter than three characters, you must add additional characters
surname	[a-zA-Z0-9]	3	32	C (M for CFT/AFT)	The recipient's Last Name, if shorter than three characters, you must add additional characters
address.line_1				C (M for AFT)	
address.city				C (M for AFT)	
address.state				C (M for AFT in US & Canada onlyinal)	
address.country_code				C (M for AFT)	

Object Name: redirect_urls

Field Name	Type	Min	Max	M/O/C	Description
success_url	URL	0	1024	C (M for Payout)	The URL to which the user is redirected in the event of a successful transaction
cancel_url	URL	0	1024	C (M for Payout)	The URL to which the user is redirected in the event of a cancelled transaction
fail_url	URL	0	1024	C (M for Payout)	The URL to which the user is redirected in the event of a failed transaction
pending_url	URL	0	1024	C (M for Payout)	The URL to which the user is redirected in the event of a pending transaction

Object Name: routing

Field Name	Type	Min	Max	M/O/C	Description
request_processor	[a-zA-Z0-9]	0	9	0	Indicates the selected processor for the specific transaction. The transaction is routed according to the transmitted value. Possible values: <ul style="list-style-type: none"> • CREDORAX • PIVOTAL • ISRACARD • LEUMICARD • CAL • NBK
requested_processor_mid	[a-zA-Z0-9]	0	32	0	Indicates the processor target MID for the specific transaction. The transaction is routed according to the transmitted value.
routing_order	[1-9]	1	2	0	The routing sequence number

Object Name: fraud

Field Name	Type	Min	Max	M/O/C	Description
active	[A-Z]	4	5	O	Boolean field specifying whether the fraud-protection service check should be bypassed. Default value is FALSE (Send to fraud check). Only available to merchants using the Smart Guard fraud-protection service.
threshold	[0-9]	0	4	O	Sets an ad-hoc threshold for the specific transaction. The threshold must be a value between 0 and 1000. Only available to merchants using the Smart Guard Plus fraud-protection service.
3d_threshold	[0-9]	1	3	O	Assigns an ad-hoc threshold that extends the regular fraud threshold, for authorised 3D secure transactions only.

Object Name: browser_info

Field Name	Type	Min	Max	M/O/C	Description
user_agent	[a-zA-Z0-9]	5	300	O	Exact content of the HTTP user-agent header.
accept_language	[a-zA-Z,]	5	16	O	Accept-Language header, comma-separated set of locales
version	[a-zA-Z0-9]	1	64	O	Browser version

Object Name: device_info

Field Name	Type	Min	Max	M/O/C	Description
type	[a-zA-Z0-9]	1	64	O	Device type (mobile, tablet, iPad, desktop, etc.)
os_name	[a-zA-Z0-9]	1	64	O	Device Operating System name

Field Name	Type	Min	Max	M/O/C	Description
os_version	[a-zA-Z0-9]	1	64	0	Device Operating System version

Appendix A: SHA512 Transaction Signature

Every APM request is associated with a package signature sent as an Authentication header in order to ensure the authenticity of data transfer. This package signature, in turn, contains the SHA512 hash of all the request values and the merchant's unique secret key.

Calculating the Signature

1. Apply the HMAC-SHA512 hashing algorithm to the JSON body of the request and the merchant's secret key.
2. Append the result of step 1 to the request's *authentication* header

Signature Calculation Example

Here is an example of how the signature is calculated using the following original request, with the secret key being: "secret":

```
{
  "payment_method": "paypal",
  "request_id": "123456789",
  "merchant_info": {
    "gw_mid": "Aa23456"
  },
  "amount": {
    "amount": "5000",
    "currency": "EUR"
  }
}
```

In this example, the JSON indentation is composed of 4 spaces.

The result of applying HMAC-SHA512 to the request body and secret is:

```
880e84253f081ff5dd4209dc0e7f82f859aca7261c95668563492097f1080e5d35de838f8d97da5e9da
a90d2a74d7aac2b07d605e4f4d004974a3579531b6bdc
```


Appendix B: Operation Result Codes

This appendix lists all the possible result codes that can returned in the “result” object and their corresponding descriptions:



Note:

The response code is 3 digits in length, and the first digit can be changed. This is done for internal purposes

Result Description	Result Code
Transaction processed successfully.	*00
Transaction has been denied.	*01
Transaction has been denied by the Gateway due to its high fraud risk.	*02
Rejected. Fraud Service is unavailable.	*03
Rejected. Bypassing the Fraud Service is not allowed.	*04
Rejected. Overriding the Fraud Threshold is not allowed.	*05
Rejected. Risk score is above limit.	*06
Transaction timeout.	*07
Transaction has been denied. Duplicate transaction.	*08
Transaction failed due to too many requests.	*09
Transaction failed due to a technical reason.	*10
The transaction in question is currently being processed. Please try again.	*11
At least one of the input parameters is malformed. Parameter [X] is invalid.	*12
At least one of the input parameters is missing. Parameter [X] is missing.	*14
Transaction denied. Invalid account.	*15
Authentication failed due to invalid authentication credentials.	*16
Payment Method not allowed for this merchant.	*18
Operation not allowed for this merchant.	*20
Invalid Payment Method.	*21
Payment Method missing.	*22
Transaction Amount not within pre-defined threshold.	*50
Insufficient funds.	*51

Result Description	Result Code
Transaction Amount exceeds or does not match the Transaction amount referenced in the request.	*52
Amount exceeds the Transaction Amount referenced in the request.	*53
Expired card.	*54
The grand total amount does not match the item total amount.	*55
The operation on the transaction referenced in the request has already been executed successfully.	*64
Referral operation not allowed.	*66
Could not find the original transaction. Make sure that it exists and that its details were transmitted correctly.	*67
Bank Account validation failed.	*80
Partial capture for Debit card: Sale succeeded; Void failed	*86
Partial capture for Debit card: Sale failed; Void succeeded	*87
Partial capture for Debit card: Sale failed,; Void failed	*88
The user aborted the payment process.	*98
Transaction is pending.	*99

Appendix C: Available Payment Methods

This appendix lists the currencies and countries supported by each payment method.

APM	Payment Method Value	Supported Currencies	Permitted Shopper Countries	Refund
7eleven		MYR	MY	No
Alfamart via DOKU		IDR	ID	No
Alipay In-Store		CHF, DKK, EUR, GBP, NOK, SEK	AT, BE, BG, CY, CZ, DE, DK, EE, ES, FI, FR, GR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK, GB	Yes
Alipay Online	alipay	AUD, CAD, CHF, CNY, EUR, GBP, JPY, HKD, NZD, SGD, USD	CN	Yes
Apple pay	applepay	All	All, subject to the scheme acceptance policy	Yes
Bancontact	bancontact	EUR	BE	Yes
Bitpay	bitpay	EUR, GBP, USD	Worldwide, except: Algeria, Bangladesh, Bolivia, Cambodia, Crimea, Cuba, Ecuador, Egypt, Indonesia, Iran, Iraq, Kyrgyzstan, Morocco, Nepal, North Korea, Pakistan, Palestinian Territory, Syria, Sudan and Vietnam.	No
Blik	blik	PLN	PL	Yes
Blik OneClick		PLN	PL	Yes
Boleto Bancário (Bradesco)		BRL	BR	Yes
Boleto Bancário (Itau)	boleto	BRL	BR	Yes
Boost		MYR	MY	yes
BRI VA via DOKU		IDR	ID	no
CIMB Niaga via DOKU		IDR	ID	no

APM	Payment Method Value	Supported Currencies	Permitted Shopper Countries	Refund
Danamon via DOKU		IDR	ID	no
DOKU Wallet		IDR	ID	no
Dragonpay		PHP	PH	no
eNETS		SGD	SG	no
EPS	eps	EUR	AT	Yes
Estonian Banks	estonianbanks	EUR	EE	No
Finnish Online Banking / Verkkopankki	verkkopankki	EUR	FI	Yes
FPX		MYR	MY	yes
Giropay	giropay	EUR	DE	Yes
Google pay	googlepay	All	All, subject to the scheme acceptance policy	Yes
GoPay		IDR	ID	yes
GrabPay (MY)		MYR	MY	yes
GrabPay (SG)		SGD	SG	yes
iDeal	ideal	EUR	NL	Yes
Indomaret via DOKU		IDR	ID	no
Jenius via DOKU		IDR	ID	no
Klarna (Financing by Card)		GBP	GB	yes
Klarna (Financing)		EUR, GBP, NOK, SEK, DKK	AT, BE, ES, FI, FR, SE, DE, NO, DK, GB	yes
Klarna (Pay Later)		CHF, GBP, EUR, NOK, SEK, DKK	AT, BE, CH, DK, ES, FI, FR, DE, IT, NL, NO, SE, GB	yes
Klarna Pay Now		CHF, EUR, SEK	AT, BE, CH, DE, ES, IT, NL, SE,	yes
Konbini		JPY	JP	no

APM	Payment Method Value	Supported Currencies	Permitted Shopper Countries	Refund
Kredivo via DOKU		IDR	ID	No
Latvian Banks	latvianbanks	EUR	LV	No
LinkAja via DOKU		IDR	ID	no
Lithuanian Banks	lithuanianbanks	EUR	LV	No
Mandiri Bank via DOKU		IDR	ID	no
Maxima	maxima	EUR	LT	No
MayBank via DOKU		IDR	ID	no
MobilePay	mobilepay	DKK, EUR, NOK, SEK, USD, GBP	All EU, EEA countries (including GB)	Yes
Multibanco	multibanco	EUR	PT	Yes
MyBank	mybank	EUR	IT	Yes
Narvesen		EUR	LT	no
OVO via DOKU		IDR	ID	no
OXXO Direct		MXN	MX	yes
Pay by Bank app		GBP	GB	yes
Payconiq		EUR	BE, LU	yes
Pay-easy		JPY	JP	No
Paypal	paypal	AUD, BRL, CAD, CZK, DKK, EUR, HKD, HUF, JPY, MYR, MXN, NOK, NZD, PHP, PLN, GBP, RUB, SGD, SEK, CHF, TWD, THB, USD	Global, except: AF,AO,BA,CD,CG,CG,CU,ER,GN,GW,GY, HT,IQ,IR,KP,LA,LY,MM,PK,SD,SO,SS,SY, TM,UG,UZ,VU,YE,ZW	Yes
Paypost	paypost	EUR	LT	No
Paysafecard	paysafecard	AUD, CAD, CHF, EUR, GBP, NOK, PLN, RON, SEK, USD	AT, AU, BE, BG, CA, CH, CY, CZ, DE, DK, ES, FI, FR, GB, GR, GE, GI, HR, HU, IE, IT, LI, LT, LU, MT, MX, NL, NO, NZ, PE, PL, PT, RO, SE, SI, SK, UY	Yes

APM	Payment Method Value	Supported Currencies	Permitted Shopper Countries	Refund
Paysafecash	paysacecash	EUR, RON, HUF, CZK, PLN, GBP, CAD, CHF, SEK, USD	AT, BE, BG, CA, CH, CY, CZ, ES, FR, GB, GR, HR, HU, IE, IT, LT, LU, LV, MT, NL, PL, PT, RO, SE, SI, SK	Yes
Paysera	paysera	EUR	EE, LT, LV	No
PayU	payu	CZK, PLN	CZ, PL	Yes
Perlas Terminals	perlas	EUR	LT	No
Permata via DOKU		IDR	ID	no
Postfinance (YellowPay)		CHF, EUR	CH	yes
Przelewy24	p24	EUR, PLN	PL	Yes
Safetypay	safetypay	USD	BR, CL, EC, MX, PE	Yes
Satispay		EUR	IT, BE, DE, FR, LU	yes
SEPA Direct Debit		EUR	AD, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LI, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, VA	yes
Skrill	skrill	EUR, GBP, USD	Global	Yes
Sofort	sofort	EUR, GBP, CHF	DE, NL, BE, AT, ES,, PL, GB, CH	Yes
Tesco Lotus		THB	TH	no
ThaiBanks		THB	TH	no
Touch 'n Go		MY	MY	yes
Trustly	trustly	CZK, DKK, EUR, GBP, NOK, PLN, SEK	AT, CZ, DE, DK, EE, ES, FI, GB, LV, LT, NL, NO, PL, SE, SK	Yes
Unionpay SecurePay		USD, EUR, HKD, SGD, CNY, CAD, GBP, CHF, AUD, NZD, JPY	CN, AU, JP, KR, NZ, SG, HK, MO, MY, TH, PH, ID, BN, VN, KH, PF, BD, NP, LK, MN, DE, FR, GB, HU, IT, GE, RU, TR, US, CA, SR, EC, DM, AZ, KG, TJ, MU, KE, SC, MG, ZA, NG, GH, KZ	Yes
WeChat Pay	wechatpay	EUR, USD, GBP, CHF, CNY	CN	Yes
WeChat Pay In-Store		EUR, USD, GBP, CHF	CN	Yes

Appendix D: SCA & 3D Secure

This section describes the specifications for using the Shift4 Payment Gateway 3D Secure service. If you are using a third-party 3D Secure service, prior to sending the transaction to Shift4 Payment Gateway, please refer to [Appendix E: How to provide 3D secure Authentication Data](#).

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.

Shift4 Payment Gateway offers two modules of 3D Secure:

- Standard 3D Secure
- 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:



- Shift4 3D Secure service supports all versions of the 3D Secure protocol, including: 3D Secure 1.0, 2.0, 2.1.0, and 2.2.0
- To use Shift4 3D Secure service, you must be registered to the service and have it activated on your account.

Contact your Shift4 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 assess 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 Shift4 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 Shift4 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 more steps to complete the transactions
- For the challenge flow, consider implementing the notification mechanism to automatically retrieve updates on the transaction processing progress without having to initiate another API call to the gateway. Contact your Shift4 account manager for more details on how to enroll to this service.

Initiating the 3D Secure process

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

The 'threed_secure.initiate' parameter can have one of the following values:

Value	Description
01	Initiate 3D Secure before completing the payment
02	Process payment without 3D Secure
03	Initiate 3D Secure according to the 3DS Adviser result (see 3DS Adviser)

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, then it can go through any of the standard 3D Secure flows.

Standard 3D Secure Workflow

Once the 3D Secure workflow is initiated in a transaction the process can go through one of 4 possible sub-workflows:

- No challenge (frictionless experience)
- Device fingerprint assessment only (frictionless experience)
- Cardholder challenge only (without device fingerprint)

- Full authentication (both device fingerprint assessment and cardholder challenge)

The entities participating in the 3D secure process are:

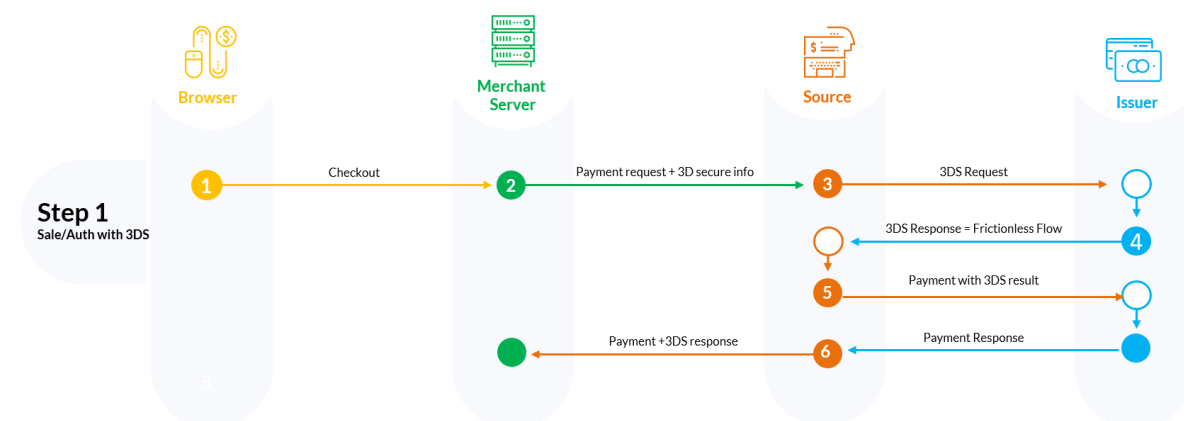
Entity	Description
Browser	The cardholder's browser from which the process was initiated
Merchant Server	The merchant's server side
Shift4	Shift4's Payment Gateway
Issuer	The issuer of the card used in the transaction

Flow A: No challenge (frictionless experience) flow

In this flow the cardholder is authenticated based on the information provided on the transaction itself, without any additional authentication (such as device fingerprint or other challenge method).

**Note:**

The more user information you provide on the initial transaction, the more likely it is that the cardholder will not have to go through additional authentication steps. See the [full list of additional recommended parameters](#)



Step 1: Cardholder goes through the checkout process on the Merchant's website.

Step 2: Merchant sends a payment request with the required 3D secure parameters to the Shift4 Payment Gateway.

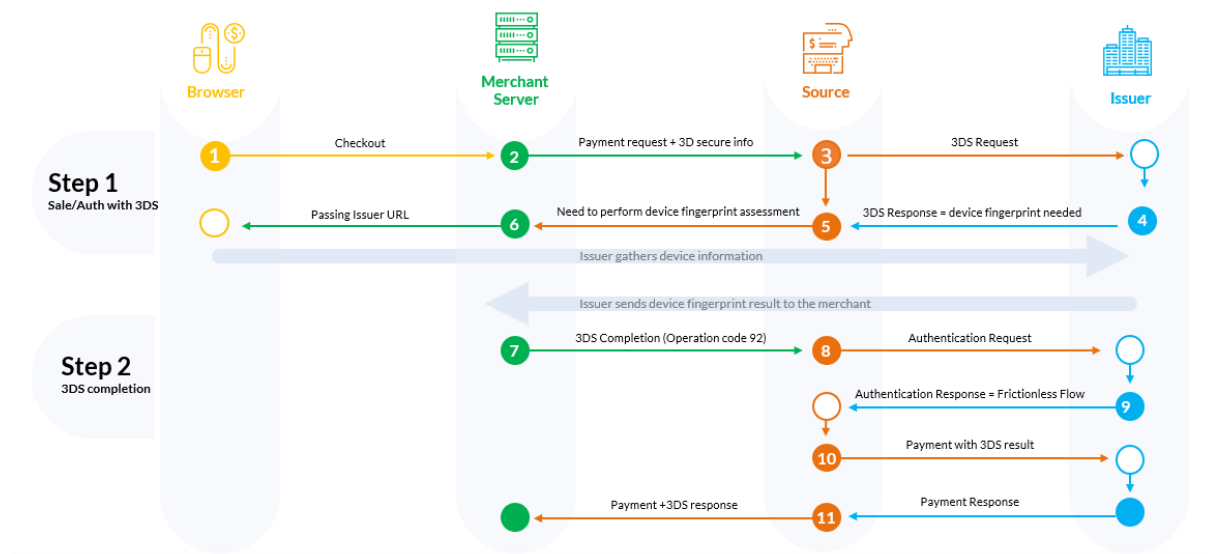
Steps 3-4: Shift4 initiates the 3D secure authentication process and receives a response from the issuer that no further authentication is required

Step 5: Shift4 instructs the issuer to perform the payment and receives the issuer response for the transaction

Step 6: Shift4 sends the transaction response with the result of the payment and the 3D secure process.

Flow B: 3D secure process requires device fingerprint assessment

In this scenario the issuer requests more information about the device that initiated the transaction (depending on the issuer this can be the cardholder's browser or other information used for risk analysis). The information is transferred electronically without the cardholder experiencing any change in the flow (frictionless experience).



Step 1: Cardholder goes through the checkout process on the Merchant's website.

Step 2: Merchant sends a payment request with the required 3D secure parameters to Shift4 Payment Gateway.

Steps 3-5: Shift4 initiates the 3D Secure process and receives from the issuer the request for device fingerprint information.

Steps 6-7: Merchant initiates the device fingerprint process. Refer to the [Device fingerprint information retrieval flow](#) for more details

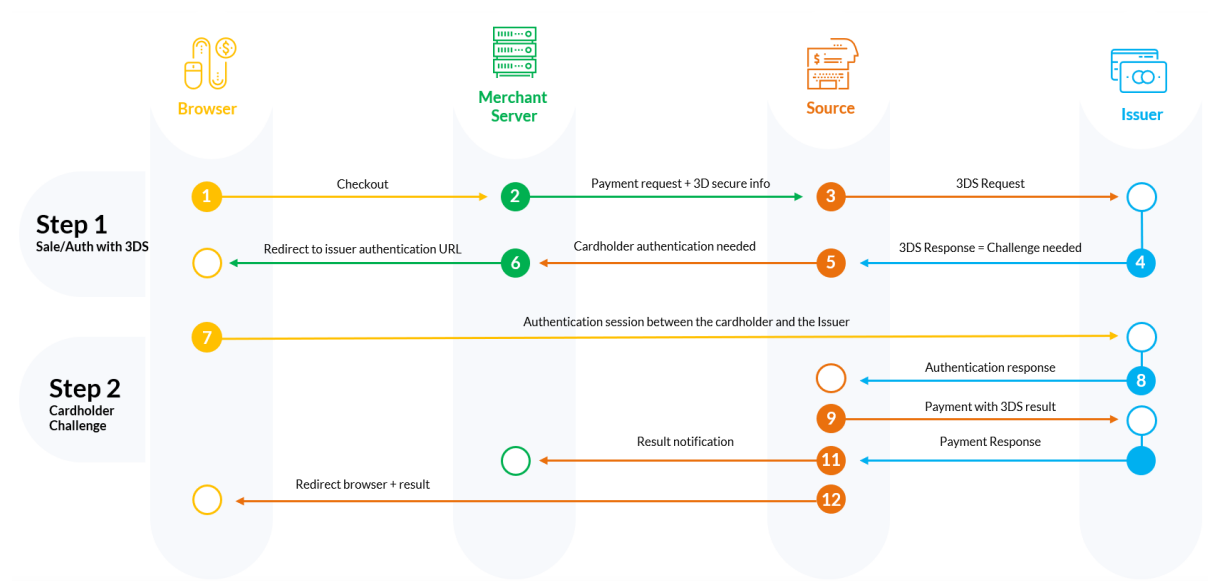
Steps 8-9: Shift4 re-initiates the 3D secure authentication process with the input received through the 3DS completion URL (/3dsmethod/{transaction_id}), and receives the authentication result from the issuer

Step 10: Shift4 initiates the payment

Step 11: Shift4 sends back to the merchant a response to the transaction initiated by operation [92] with the result of the payment and the 3D secure process.

Flow C: 3D secure requires a user challenge flow (redirection to issuer)

In this scenario the issuer requires a user challenge flow where the cardholder is prompted with an authentication screen.



Step 1: Cardholder goes through the checkout process on the merchant's website.

Step 2: Merchant sends payment request with 3D secure to Shift4 Payment Gateway

Steps 3-4: Shift4 Payment Gateway initiates the 3D secure authentication process. Cardholder authentication is needed.

Step 5: Shift4 responds to the merchant with the URL for the authentication process. In the response the transaction status is listed as 'pending'.

Steps 6-7: Merchant initiates the authentication process in the cardholder's browser. See [Cardholder challenge flow](#) for more details.

Steps 8-9: Shift4 receives the authentication results from the Issuer.

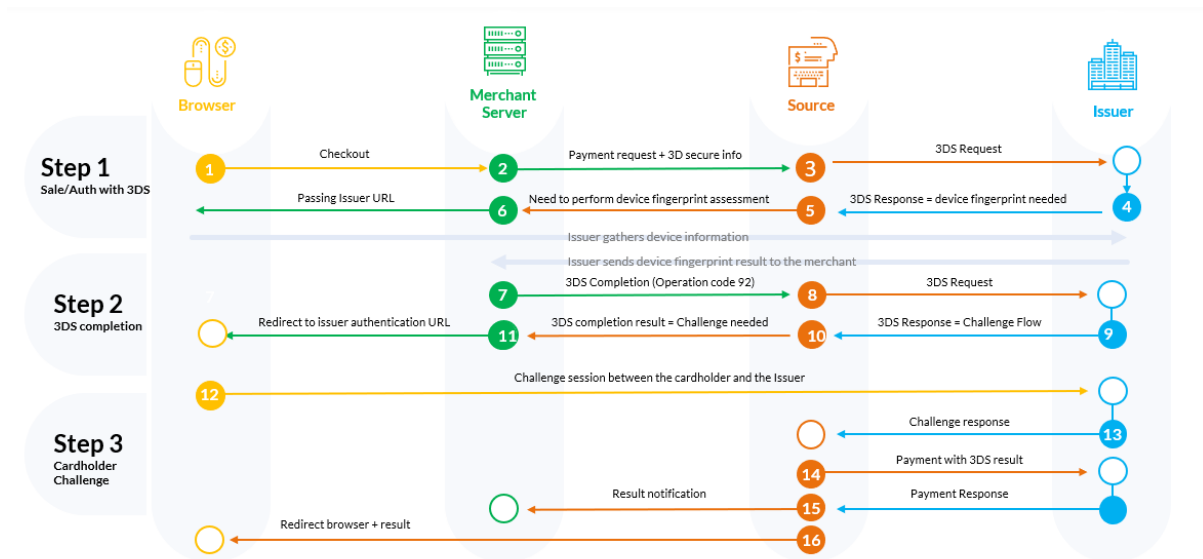
Step 10: Shift4 initiates the payment

Step 11: Shift4 sends notification to the merchant with all payment & authentication results.

Step 12: Shift4 redirects the browser to the merchant site.

Flow D: 3D secure flow requires fingerprint authentication and user challenge

This scenario requires full authentication of the cardholder with both fingerprint flow and cardholder challenge.



Step 1: Cardholder goes through the checkout process on the Merchant's website.

Step 2: Merchant sends a payment request with the required 3D secure parameters to the Shift4 Payment Gateway.

Step 3-5: Shift4 initiates the 3D Secure process and receives from the issuer the request for device fingerprint information.

Step 6-7: Merchant initiates the device fingerprint process. Refer to [device fingerprint information retrieval flow](#) for more details.

Step 8-9: Shift4 re-initiates the 3D secure authentication process with the input received through the 3DS completion URL (`/3dsmethod/{transaction_id}`), and receives the authentication result from the issuer.

Step 10: Shift4 responds to the merchant with the URL for the authentication process. In the response the transaction status is listed as 'pending'.

Step 11-12: Merchant initiates the authentication process in the cardholder's browser. See [Cardholder challenge flow](#) for more details.

Step 13: Shift4 receives the authentication results from the Issuer.

Step 14: Shift4 Payment Gateway initiates the payment

Step 15: Shift4 sends notification to the merchant with all payment & authentication results.

Step 16: Shift4 redirects the browser to the merchant site.

Device fingerprint information retrieval flow

When device fingerprint assessment is required by the issuer, Shift4 responds with the following parameters:

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

1. Upon receiving the above parameters, create a JSON object with the 3DS Method Data elements:

```
threedSMMethodNotificationURL = <the URL to which the issuer will send his approval>
threedSServerTransID = <threed_secure.trxid >
```

2. Encode the JSON object in Base64 URL encoding.
3. Render a hidden HTML iframe in the Cardholder's browser and send a form with a field named threeDSMethodData containing the **URL friendly** Base64url JSON Object via HTTP POST to the threed_secure.threedsmethod URL you received from Shift4.
4. At this stage you should get a response about the completion of the fingerprint collection process. The information is a POST response to the notification URL you provided in the threeDSMethodNotificationURL parameter in step 1. It contains a single encoded parameter called threeDSMethodData.

Take note: If the notification is received within 10 seconds, then when executing the next step, set threed_secure.completion_ind = Y; otherwise, set threed_secure.completion_ind = N.

5. Use the information from the response to send a completion call to Shift4. This is done by sending the 3DS completion to /3dsmethod/{transaction_id} with the following parameters:

Name	Description	Type	Length	M/O/C
merchant_info. gw_mid	Shift4 assigned gateway Merchant ID	[A-Z0-9_]	3,6	m
request_id	Request ID A unique transaction reference number. It should be unique to each transaction and to each MID. May be used when corresponding with the payment processor or reconciling transactions.	[a-zA-Z0-9-]	1,32	m

Name	Description	Type	Length	M/O/C
	Note: No plaintext cardholder data should be provided in this field.			
threed_secure.completion_ind	<p>Relevant only if <code>threed_secure.channel = 02</code>. Received as part of the 3DS completion flow. The accepted values are:</p> <ul style="list-style-type: none"> Y – Successfully completed N – Did not successfully complete U – Unavailable <p>Received from the issuer. Indicates whether the device fingerprint collection completed successfully.</p>	[Y, N, U]	1,1	m

Cardholder challenge flow

When a cardholder challenge is required by the issuer, redirect the browser to the issuer URL.

You will receive a `redirect_urls.redirect_url` parameter as part of the original payment request or as the response to 3DS Completion URL (depending on the 3D secure flow of the transaction). In order to reach the issuer's side, open a dynamic iFrame on the browser side, and refer to the address received in the `redirect_urls.redirect_url` parameter. However, for a 3DS 1.0 protocol, it is recommended to redirect to the address received in the `redirect_urls.redirect_url` parameter instead of using an iFrame since not all issuers support this functionality.

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
fraud_service.threed_secure_threshold	[0-9]	1	3	Assigns an ad-hoc threshold that extends the regular fraud threshold, for authorised 3D secure transactions only.

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
threed_secure.smart_3d.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
threed_secure.smart_3d.result_reason	[a-zA-Z0-9]	0	128	Includes the rule id which was executed as part of the Smart 3D rule engine

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 card
- 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
threed_secure.exemption.action	[0-9]	o	2,2	Indicates the merchant preference regarding SCA exemption. Possible values are:

Name	Type	o/m	Min, Max	Description
				<p>01: Do not request exemption. This is the default behaviour for the Shift4 Gateway. If the field is absent from the transaction request, no exemption will be applied.</p> <p>02: Request an exemption as part of the payment request.</p> <p>03: Request an exemption as part of the 3D Secure request</p> <p>04: Request exemption by default. Shift4 will apply for exemption as part of the 3D Secure request if possible.</p> <p>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.</p>
threed_secure.exemption.reason	[0-9]	o	2,2	<p>This field is required when <i>exemption.action</i> = 02 or 03.</p> <p>Possible values:</p> <p>01: Low value transaction (below 30 EUR or equivalent)</p> <p>02: Low risk transaction (TRA)¹</p> <p>03: Request Trusted Beneficiary Indicator (<i>Whitelisting</i>)²</p> <p>04: Secure Corporate Cards ³</p> <p>05: Delegated Authentication ⁴</p> <p>06: MIT – Recurring same amount</p> <p>07: MIT – other ⁵</p> <p>08: Trusted Beneficiary Indicator (<i>Whitelisting</i>) – Done⁶</p> <p>¹ Requires real-time fraud monitoring solutions</p> <p>² Use this value to indicate to the ACS to obtain confirmation from the cardholder to whitelist the merchant for future purchases</p> <p>³ This is not a standard exemption you can request. If you know the card used for the</p>

Name	Type	o/m	Min, Max	Description
				<p>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.</p> <p>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.</p> <p>⁵ Any MIT transaction must be sent with this flag to make sure the transaction will not require SCA.</p> <p>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.</p>
three_secure.exemption.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 <code>exemption.reason = 02</code>

Managing SCA for Merchant initiated transaction

Merchant initiated transactions can be part of two different business cases:

- **Recurring transactions:** 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.
- **Periodic charges:** always initiated by the merchant, based on card details provided by the cardholder (for example, the cardholder provided their card details to pay for utility bills). In this case the cardholder is authenticated with SCA when they first provide the card, and all subsequent payments will be out of scope.

For a merchant-initiated transaction to be exempted of SCA, you must include the value of the "initial transaction ID" (received as part of the first authenticated transaction) with every subsequent transaction you initiate, in any of the above scenarios.

Exemption – Response Parameters

Name	Type	m/o	Min,Max	Description
threed_secure.white_list_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 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 probability for a frictionless experience for the cardholder.

Recommended Parameters

To increase the probability for a frictionless 3D secure flow, it is **recommended** that each request contain as many of the following list of parameters as possible:

Requested Data	Shift4 Parameters	Description
Browser IP address	shopper_info.ip_address	IP address of the browser as returned by the HTTP headers. In either ipv4 or ipv6 format
Buyer email address	shopper_info.email	Cardholder's email address in valid email address format, such as <i>joe@bloggs.com</i>
Billing Information	billing_address.line_2	Cardholder Billing Address street number
	billing_address.line_1	Cardholder Billing Address street name
	billing_address.city	Cardholder Billing Address city name
	billing_address.state	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 .
	billing_address.country_code	Cardholder Billing Address Country Code. Please refer to ISO 3166-1-alpha-2 for a list
	billing_address.postal_code	Cardholder Billing Address Postal/ZIP Code

Requested Data	Shift4 Parameters	Description
Shipping information	shipping_address.city	City of the shipping address requested by the Cardholder
	shipping_address.country	Country of the shipping address requested by the Cardholder. Please refer to ISO 3166-1-alpha-2 for a list
	shipping_address.line_1	First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase
	shipping_address.line_2	Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase
	shipping_address.postal_code	ZIP or other postal code of the shipping address associated with the card used for this purchase
	shipping_address.state	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?	three_d_secure.cardholder_addr_match	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 (`three_d_secure.initiate = 01` or `03`):

Name	Description	Type	m in	max	m/o/c
three_d_secure.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
three_d_secure.redirect_url	Contains the merchant URL to which the browser should be redirected after the challenge session	URL	0	2048	m
three_d_secure.category	Identifies the category of the message for a specific use case. The accepted values are:	[0-3]	2	2	o

Name	Description	Type	min	max	m/o/c
	01 - PA (Payment authentication) 02 - NPA (NON-payment authentication) 80 – Data only (Mastercard only, valid only for threed_secure.channel = 01 or 02)				
threed_secure.completion_ind	Relevant only if <code>threed_secure.channel = 02</code> . Received as part of the 3DS completion flow. The accepted values are: Y – Successfully completed N – Did not successfully complete U – Unavailable	[YNU]	1	1	c (m when <code>threed_secure.channel = 02</code>)
threed_secure.sdk.interface	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 <code>threed_secure.channel=01</code> (APP).
threed_secure.sdk.ui_types	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 <code>threed_secure.channel=01</code> (APP).
threed_secure.threeds_requestor.threeds_requestor_authentication_info.threeds_req_auth_method	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)	[0-6]	2	2	o

Name	Description	Type	min	max	m/o/c
	<p>02 - Login to the cardholder account at the merchant system using merchant's own credentials</p> <p>03 - Login to the cardholder account at the merchant system using federated ID</p> <p>04 - Login to the cardholder account at the merchant system using issuer credentials</p> <p>05 - Login to the cardholder account at the merchant system using third-party authentication</p> <p>06 - Login to the cardholder account at the merchant system using FIDO Authenticator</p> <p>07 - Login to the cardholder account at the merchant system using FIDO Authenticator (applicable for 3DS version 2.2 and above)</p> <p>08 - SRC Assurance Data. (applicable for 3DS version 2.2 and above)</p>				
three_secure.threeds_requestor.threeds_requestor_authentication_info.threeds_req_auth_timestamp	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
three_secure.threeds_requestor.threeds_requestor_authentication_info.threeds_req_auth_data	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
three_secure.threeds_requestor.threeds_requestor_challenge_ind	Indicates whether a challenge is requested for this transaction. For example: For three_secure.category 01-PA, a merchant may have concerns about the transaction, and request a challenge. For three_secure.category 02-NPA, a challenge may be necessary when adding a new card to a wallet. 01 - No preference	[0-4]	2	2	o

Name	Description	Type	min	max	m/o/c
	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)				
thread_secure.thread_s_re questor.thread_s_reusto r_prior_authentication_inf o.thread_s_req_prior_ref	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
thread_secure.thread_s_re questor.thread_s_reusto r_prior_authentication_inf o.thread_s_req_prior_auth _method	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
thread_secure.thread_s_re questor.thread_s_reusto r_prior_authentication_inf o.thread_s_req_prior_auth _timestamp	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
threed_secure.threeds_requestor.threeds_requestor.prior_authentication_info.threeds_req_prior_auth_data	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.	[a-zA-Z0-9]	0	2048	o
threed_secure.threeds_requestor.threeds_requestor.dec_req_ind	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.	[YN]	1	1	o
threedSecure.threeds_requestor.threeds_requestor.dec_max_time	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
threed_secure.cardholder_account.acctinfo.chacc_date	Date that the cardholder opened the account with the merchant. Date format = YYYYMMDD.	[0-9]	8	8	o
threed_secure.cardholder_account.acctinfo.chacc_change_ind	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
threed_secure.cardholder_account.acctinfo.chacc_change	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
threed_secure.cardholder_account.acctinfo.chacc_pw_change_ind	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
threed_secure.cardholder_account.acctinfo.chacc_pw_change	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
threed_secure.cardholder_account.acctinfo.ship_address_usage_ind	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
threed_secure.cardholder_account.acctinfo.ship_address_usage	Date when the shipping address used for this transaction was first used. Date format must be YYYYMMDD.	[0-9]	8	8	o
threed_secure.cardholder_account.acctinfo.txn_activity_day	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
threed_secure.cardholder_account.acctinfo.txn_activity_year	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

Name	Description	Type	min	max	m/o/c
threed_secure.cardholder_account.acctinfo.provision_attempts_day	Number of Add Card attempts in the last 24 hours.	[0-9]	0	10	o
threed_secure.cardholder_account.acctinfo.nbpurchase_account	Number of purchases with this cardholder account during the previous six months.	[0-9]	0	10	o
threed_secure.cardholder_account.acctinfo.suspicious_acc_activity	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
threed_secure.cardholder_account.acctinfo.ship_name_indicator	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
threed_secure.cardholder_account.acctinfo.payment_acc_ind	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
threed_secure.cardholder_account.acctinfo.payment_acc_age	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
threed_secure.cardholder_account.acc_id	Additional information about the account optionally provided by the merchant.	[a-zA-Z0-9]	0	64	o

Name	Description	Type	m in	max	m/o/c
threed_secure.cardholder_account.pay_token_ind	This field has a value of "true" if the transaction was de-tokenised prior to being received by Shift4.	[a-z]	4	5	O
threed_secure.cardholder_addr_match	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical. Accepted values: <ul style="list-style-type: none"> • 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
threed_secure.white_list_status	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
shopper_info.home_phone.country	Country Code of the home phone.	[0-9]	1	3	c (m if shopper_info.home_phone.number_exists)
shopper_info.mobile_phone.number	The mobile phone provided by the Cardholder, without the country code	[0-9]	0	18	O
shopper_info.mobile_phone.country	Country Code of the mobile phone.	[0-9]	1	3	c (m if shopper_info.mobile_phone.number_exists)
shopper_info.work_phone.number	The work phone provided by the Cardholder, without the country code	[0-9]	0	18	O
shopper_info.work_phone.country	Country Code of the work phone.	[0-9]	1	3	c (m if shopper_info.work_phone.number_exists)
shipping_address.city	City of the shipping address requested by the Cardholder.	[a-zA-Z]	3	32	O

Name	Description	Type	min	max	m/o/c
shipping_address.country	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 shipping_address.state exists or if shipping information is not the same as billing information
shipping_address.line_1	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	c m – when thread_secure.cardholder.address_match = false
shipping_address.line_2	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 thread_secure.cardholder.address_match = false
shipping_address.postal_code	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 thread_secure.cardholder.address_match = false
shipping_address.state	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]	1	3	o m – when thread_secure.cardholder.address_match = false
thread_secure.purchase_merchant_risk_indicator.shipping_indicator	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	[0-7]	2	2	o

Name	Description	Type	min	max	m/o/c
	<p>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:</p> <p>01 - Ship to cardholder's billing address</p> <p>02 - Ship to another verified address on file with merchant. In this case, shipping information is required even though <code>threed_secure.cardholder.addr_match = true</code>.</p> <p>03 - Ship to address that is different from the cardholder's billing address. In this case, shipping information is required even though <code>threed_secure.cardholder.addr_match = true</code>.</p> <p>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 <code>threed_secure.cardholder.addr_match = true</code>.</p> <p>05 - Digital goods (includes online services, electronic gift cards and redemption codes)</p> <p>06 - Travel and Event tickets, not shipped</p> <p>07 - Other (for example, Gaming, digital services not shipped, emedia subscriptions, etc.)</p>				
<code>threed_secure.purchase.merchant_risk_indicator.deliver_timeframe</code>	<p>Indicates the merchandise delivery timeframe. Accepted values are:</p> <p>01 - Electronic Delivery</p> <p>02 - Same day shipping</p> <p>03 - Overnight shipping</p> <p>04 - Two-day or more shipping</p>	[0-4]	2	2	o

Name	Description	Type	m in	max	m/o/c
threed_secure.purchase.merchant_risk_indicator.deliver_email_address	For electronic delivery, the email address to which the merchandise was delivered.	email	7	64	o
threed_secure.purchase.merchant_risk_indicator.reorder_items_ind	Indicates whether the cardholder is reordering previously purchased merchandise. Accepted values are: 01 - First time ordered 02 - Reordered	[0-2]	2	2	o
threed_secure.purchase.merchant_risk_indicator.preorder_purchase_ind	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
threed_secure.purchase.merchant_risk_indicator.preorder_date	For a pre-ordered purchase, the expected date that the merchandise will be available. Date format must be YYYYMMDD.	[0-9]	8	8	o
threed_secure.purchase.merchant_risk_indicator.gift_card_amount	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
threed_secure.purchase.merchant_risk_indicator.gift_card_curr	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
threed_secure.purchase.merchant_risk_indicator.gift_card_count	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
threed_secure.purchase.purchase_date	Date and time of the purchase expressed in UTC. The field is limited to 14 characters, formatted as YYYYMMDDHHMMSS.	[0-9]	14	14	m
threed_secure.purchase.recurring_expiry	Date after which no further authorisations shall be performed. This field is limited to	[0-9]	8	8	c

Name	Description	Type	min	max	m/o/c
	8 characters, and the accepted format is YYYYMMDD. This field is required if payment_details.recurring=1 or 2				
threed_secure.purchase.recurring_frequency	Indicates the minimum number of days between authorisations. The field is limited to 4 characters. This field is required if payment_details.recurring =1 or 2	[0-9]	0	4	c
threed_secure.purchase.transaction_type	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
threed_secure.merchant_name	Assigned merchant name (with a prefix of "http://" or "https://")	[a-zA-Z0-9]	1	25	o
browser_info.browser_accept_header	Exact content of the HTTP accept headers.	[a-zA-Z0-9]	0	2048	o m if threed_secure.channel =02
shopper_info.ip_address	IP address of the browser as returned by the HTTP headers. Supports both ipv4 & ipv6 formats.	ip	7	48	o m for Visa 3D Secure transactions m if threed_secure.channel =02
browser_info.browser_java_enabled	Boolean (true/false) that represents the ability of the cardholder browser to execute Java. This field is required for requests where threed_secure.channel = 02 (Browser).	[a-z]	4	5	o m if threed_secure.channel =02

Name	Description	Type	m in	max	m/o/c
browser_info.browser_java_script_enabled	Boolean that represents the ability of the cardholder browser to execute JavaScript. Accepted values are true / false	[a-z]	4	5	o m if threed_secure .channel =02
browser_info.accept_language	Value representing the browser language as defined in IETF BCP47. For example: en-GB	[A-Za-z,-]	2	16	o m if threed_secure .channel =02
browser_info.browser_color_depth	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 threed_secure .channel =02
browser_info.browser_screen_height	Total height of the Cardholder's screen in pixels.	[0-9]	1	6	o m for Visa 3D Secure transactions m if threed_secure .channel =02
browser_info.browser_screen_width	Total width of the Cardholder's screen in pixels.	[0-9]	1	6	c m for Visa 3D Secure transactions m if threed_secure .channel =02
browser_info.browser_tz	Time difference between UTC time and the Cardholder browser local time, in minutes.	[0-9,-]	1	5	o m if threed_secure .channel =02

Name	Description	Type	min	max	m/o/c
browser_info.user_agent	Exact content of the HTTP user-agent header.	[a-zA-Z0-9]	5	300	o m if threed_secure .channel =02
browser_info.challenge_window_size	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 threed_secure .channel =02
threed_secure.sdk.sdk_apid	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 threed_secure .channel =01
threed_secure.sdk.sdk_encdata	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 threed_secure .channel =01
threed_secure.sdk.sdk_ephempubkey	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 threed_secure .channel =01
threed_secure.sdk.sdk_maxtimeout	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 threed_secure .channel =01

Name	Description	Type	min	max	m/o/c
threed_secure.sdk.sdk_referencenumber	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 threed_secure.channel =01
threed_secure.sdk.sdk_transactionid	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 threed_secure.channel =01

Response parameters

Name	Description	Type	min	max	m/o/c
threed_secure.whitelist_status_source	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

Smart 3D Secure Standalone Services

The Shift4 Gateway enables technical and business entities to use the Shift4 Smart 3D Secure service as a standalone service. The specifications below guide you on how to use Shift4 Smart 3D Secure services if you are connected to the Shift4 gateway and process transactions with other acquirers. The specifications also apply if you are connected to the Shift4 gateway for our 3D Secure services only and are interested in authentication in order to process the transactions using other gateways. Following initial setup of standalone 3D Secure to enable technical connectivity, there is no need to setup each and every business entity (merchant) that uses the service. Instead, you can send the relevant information as part of the transaction and the Shift4 gateway will successfully process the authentication request.

Initial Setup

If Credorax is not the acquirer, then in order to process non-Credorax acquirer BINs you must set up those BINs in the Shift4 systems prior to processing 3DS standalone transactions.

Please contact your Solution Architect for initial setup of standalone 3D Secure.

Providing 3DS Standalone to Multiple Merchants

If you are providing 3DS standalone to multiple merchants, then:

- **threed_secure.requestor_name** must be a unique merchant name assigned by the partner
- **threed_secure.requestor_id** must be in the following format:
 - For Visa: 10067907*[partner prefix][merchant unique ID]
 - For Mastercard: CRE51138[partner prefix][merchant unique ID] where:
 - **[Partner prefix]** is the 4-character prefix assigned by Shift4 to the partner upon onboarding **[Merchant unique ID]** is a 21-character ID generated by the partner, unique for each merchant
 - For Discover: CREDORAX_[merchant unique ID] where:
 - **[Merchant unique ID]** is a max 26-character ID generated by the partner, unique for each merchant

Using 3DS Standalone as a Single Merchant

If you are a merchant using 3DS standalone yourself, and not providing it to others, then in the course of initial setup Shift4 will provide you with both of the following:

- **threed_secure.requestor_name**
- **threed_secure.requestor_id**

Appendix E: How to Provide 3D Secure Authentication Data

This section describes the specifications of the `threed_secure` parameters 'eci', 'cavv', 'xid', used when running 3D secure with a third-party provider. If you are using the Shift4 Payment Gateway 3D Secure service, please refer to [Appendix D: SCA & 3D Secure](#).

3D secure data is transmitted via the following parameters:

- `threed_secure.eci` - ECI (Electronic Commerce Indicator)
- `threed_secure.cavv` - CAVV/AAV
- `threed_secure.xid` – XID

Note:



If you have more than one payment processor configured with the Shift4 gateway, you must send the `routing.request_processor` parameter as part of the transaction. The value of the parameter should indicate the processor used for the 3D Secure authentication. A mismatch between the 3DS processor and the transaction processing processor may cause a transaction rejection.

If you only have one processor configured you do not have to provide the `routing.request_processor` parameter, but there should still be a match between the processor indicated in the 3DS authentication and the processor of the transaction.

ECI (Electronic Commerce Indicator)

Valid ECI values are:

ECI	Description
00	Mastercard/Maestro authentication is unsuccessful
01	Mastercard/Maestro authentication attempted
02	Mastercard/Maestro fully authenticated
05	Visa/JCB/American Express/Diners/Discover fully authenticated
06	Visa/JCB/American Express/Diners/Discover authentication attempted MasterCard/ Maestro successful authentication (see comment)
07	Visa/JCB/American Express/Diners/Discover authentication is unsuccessful or unattempted, or successfully authenticated (see comment) Mastercard/Maestro Recurring Payment fully authenticated

**Note:**

For Mastercard, the AAV is required for MCCs 7995 and 6012. For Maestro, the AAV is required for all transaction.

The XID field is optional for Mastercard / Maestro transactions with an ECI of 01, but should either be populated with a 20-byte alphanumeric transaction identifier or with 'none'.

Mastercard example:

- `threed_secure.eci=02, threed_secure.cavv=jj81HADVRtXfCBATEp01CJUAAAA=, threed_secure.xid=00000000000000000501`
- `threed_secure.eci=01, threed_secure.cavv=jj81HADVRtXfCBATEp01CJUAAAA=, threed_secure.xid=00000000000000000501`

**Note:**

- Attempted Mastercard and Maestro authenticated transaction may not exceed 10% of the total number of Secure Code transaction.
- Shift4 does not participate in the Mastercard/Maestro Advanced Registration and Maestro Recurring Payments programs, and as such does not support static AAV. The gateway will reject Secure Code transaction where the UCAF transmitted via the `threed_secure.cavv` parameter is not unique to each received transaction request

Hex-encoding for Visa

As mentioned above, we require that Visa 3D secure data be hex-encoded before transmission. Assuming the value is base-64 encoded, the hex-encoding process is carried out as follows:

1. Apply Base-64 decoding to the original value.
2. Hex-encode the resulting value
3. Transmit the result via the appropriate subfield.

Visa CAVV example:

Base-64 encoded CAVV: AAABAxZhdwAAAAMDAWF3AAAAAA=

Base-64 decoding (step 1) results in value:

aw

aw

Hex-encoding (step 2) results in value: 0000010316617700000003030161770000000000

Guidelines for 3D secure 2.0 and higher

When authentication is done using 3-DSecure 2.0 or higher:

1. The `threeed_secure.xid` parameter is not required. Instead send “none”.
2. In addition, send the following parameters as part of the request:

Parameter name	Description	Format	Min,Max
<code>threeed_secure.version</code>	Indicates the 3D Secure protocol version Possible values: <ul style="list-style-type: none">• 1.0• 2.0• 2.1.0• 2.2.0	[0-9]	3,5
<code>threeed_secure.directory.xid</code>	3DS Directory server transaction ID. Must be sent if <code>threeed_secure.version = 2.0</code> or higher and <code>threeed_secure.eci</code> , <code>threeed_secure.cavv</code> is used.	[0-9A-Za-z,-]	34

Appendix F: Setting Up MobilePay

To use MobilePay as part of your Shift4 Payment service you must be registered with MobilePay. Contact your Shift4 Account Manager to initiate this process before you want to begin processing.

You will need to provide the following details:

- Merchant name to be displayed to the end-user
- URL of your website, where you are going to offer MobilePay as a payment method
- Logo URL to be shown to the end-user during the payment
 - 250X250 pixels
 - PNG or JPG
 - Hosted using a secure HTTPS connection
 - Set content-type in the HTTP header to MIME types (e.g. image/png or image/jpeg)

End-user's minimal age: required for merchants who restrict their services or goods to a certain age

Revision History

Version	Subject /Date	Description
2.1 rev 2	May 2024	<ul style="list-style-type: none"> • Removed Poli from payment methods • Added Mandatory fields for AFT in receipt_info object: <ul style="list-style-type: none"> ◦ first_name ◦ surname ◦ address.line_1 ◦ address.city ◦ address.state ◦ address.country_code • Updated Sofort permitted shopper countries • Changed the requirement of the following fields to Mandatory for Visa 3D Secure transactions: <ul style="list-style-type: none"> ◦ shopper_info.ip_address ◦ browser_info.browser_screen_height ◦ browser_info.browser_screen_width ◦ shopper_info.phone_number ◦ shopper_info.email ◦ payment_details.cardholder_name • Added PAR field to payment_details object • Updated original_description field in result object to original_response_description
2.1 rev 1	Rebranding	Rebranding to Shift4
2.0	New feature, new objects and parameters	<ul style="list-style-type: none"> • Added new supported payment method: MobilePay • Added routing parameters • Added Stand-In parameters • Added Partial Capture (Israeli acquiring only) parameters

		<ul style="list-style-type: none">• Added seller informat
--	--	---

SHIFT

Summary of Changes

The sections below detail the changes made in each Shift4 product requirements. Refer to the sections of the Shift4 product you use for authentications to see what has changed.

For full information, refer to the documentation on our [Developer](#)

Contents

Payment Platform API	1
Alternative Payment Methods API	1
HPP Form	2
HPP Code	2
PayByLink	2

Payment Platform API

The requirement of the following fields have been changed to non-optional transactions:

- **c1** (*Cardholder's full name*)
- **c2** (*Cardholder's contact phone number*)
- **c3** (*Cardholder's email address*)
- **d1** (*Cardholder IP Address*)
- **3ds_browserscreenheight**
- **3ds_browserscreenwidth**

Alternative Payment Methods API

The requirement of the following fields have been changed to non-optional transactions:

- **shopper_info.ip_address**

Version	Subject /Date	Description
		ion object
1.9	New functionality, new objects and new parameters	<ul style="list-style-type: none"> Added 3D Secure functionality (currently applicable to Google Pay) Added token management functionality (applicable to supporting payment methods) Added payout parameters for Google Pay and Apple Pay Fixed the signature calculation example, original request and result in Appendix A Fixed SCA for merchant-initiated transactions Updated the list of supported payment methods
1.8 rev 5	Minor changes	<p>Removed the following fields from the request fields table. They are only included in the response message fields.</p> <ul style="list-style-type: none"> multibanco_entity multibanco_reference
1.8 rev 4	New objects and parameters	Added merchant advice code to Object Name: Result in Response Message Format
1.8 rev 3	Minor changes	Removed New Zealand from permitted shopper country and currency for Poli payment method
1.8 rev 2	Various fixes	Updated production URL, fixed signature encoding in Retrieval Transaction example, updated signature calculation example in Appendix A
1.8 rev 1	Payout support for APMs & API fixes	Discontinuation of payout payment methods, and correction of the authorisation API URLs
1.8	Additional Payment methods	New supported payment methods: Itau, Santander, Bradesco, Bank of Brasil, Webpay, Boleto

Version	Subject /Date	Description
1.7 rev 4	Requirement change	Changed minimum length of request_id
1.7 rev 3	Minor text fixes	Google Pay Specifications
1.7 rev 2	Minor text fixes	Updated Google Pay transaction flow Added payment methods: BLIK, Paysafecash, TrustPay Removed Zimpler payment method
1.7 rev 1	Minor changes	Added Google Pay integration information Added an accurate description of the shopper_info.mobile_phone object structure
1.7	New features, objects and parameters	Added support for Apple Pay and Google Pay Added support for additional merchant_info , purchase_info , shipping_address and result parameters Added support for the new payment_details , payment_details.fraud , routing , fraud , browser_info , and device_info objects
1.6 rev 1	Minor changes	PCI environment
1.6	New features	Added support of PF model
1.5	New Features	New supported payment methods: Paysera, Estonian banks, SafetyPay, Skrill, BitPay, Polish Payout Support of Astropay Direct integration and AstroPay Direct Payout Get Banks API – retrieve a list of supported banks in a specified country (required for AstroPay Direct)
1.4 rev 1	New Feature & fixes	Support in Alipay, Zimpler, Qiwi Fix in the description of the notification mechanism Fix in the GET example Fix in the response_code, response_description name field to match the actual API.

Version	Subject /Date	Description
1.3 rev 1	New Feature	MyBank processing Entercash processing Change in shopper_info first_name & shopper_info last_name definitions
1.2 rev 1	New Feature	Przelewy24 processing China union Pay processing
1.1 rev 1	New Feature	Sepa Payout processing Astropay Card processing Changed the transaction time to be under root in the response instead of purchase info.
1.0 rev 2	Fixes	Added information about the notification IP whitelist Changed the transaction time format

Need Support?

Contact our Client Relations Centre 24/7 for any additional information or technical issue:

US: +1.617.715.1977

UK: +44.20.3608.1288

EU: +356 2778 0876

Email: support.europe@shift4.com