SHIFT4™

Payment Page Services

PayByLink

API Specifications

Version 2.2 | November 2023

Contents

Introduction

Shift4 PayByLink is a service that allows you to create a branded, dedicated and secure payment link that is sent to your shoppers to complete their purchase, via email or text message. This link can also be embedded in other types of customer communication such as invoices or a reply email. The shopper uses the payment link, which is associated with their purchase, to complete the transaction by entering their card details on a dedicated page. This ensures that no card data is stored on or passes through your systems, significantly reducing your PCI compliance scope. The payment link's status can be tracked using the Insights customer portal or the API.

This service can be accessed through Insights or API and supports generating single or multiple payment links at a time.

The purpose of this document is to provide an in-depth description of the Shift4 PayByLink API specifications as well as the batch mode used to create multiple links at once via a CSV file uploaded to the Insights customer portal.

Useful Documents / References

The following additional documents may be helpful in understanding PayByLink:

Shift4 Payment API	The Shift4 Payment API specification provides detailed information on processing card-not-present transactions.
Form Payment Page Specifications	The Shift4 Form Payment Page API specification provides detailed information on using Shift4 payment page services
Data Transfer Specifications	The Shift4 Data Transfer Interface specification provides an in-depth description of the Data Transfer Interface and format specifications of the reports provided by Shift4.

These documents can be found on the Shift4 Developer Portal.

Intended Audience

This document is intended for merchants who wish to implement the PayByLink functionality as part of their business in order to accept payments.

Certification

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

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

Publication Identification

Overview

Introduction

The PayByLink service is part of the Shift4 service suite**.** This solution ensures that no card data passes through the merchant's website or server, nor is it stored on them. Implementing this solution can significantly reduce your PCI compliance requirements[1].

PayByLink supports authorisation requests and safe transactions as well as 3D Secure transactions.

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

Additional Supported services

Note: Each additional supported service requires registration with Shift4.

Contact your account manager for more details.

3D Secure

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

User Error Handling

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

Addresses

Integration address: https://ppskey-int.credorax.com/payments/rest/payment_link/batch/create

Production address:
https://paybylink.sourcepayments.com/payments/rest/payment_link/batch/create

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

HTTP Specifications

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

Security/Authentication

A secured channel should be used for sending redirect requests. The client is authenticated using a HMAC-SHA512 digital signature which must be sent in the request payload and used for verification before the request is approved.

See *Appendix A: SHA512 Cipher* for further details.

Batch Request using the Insights Portal

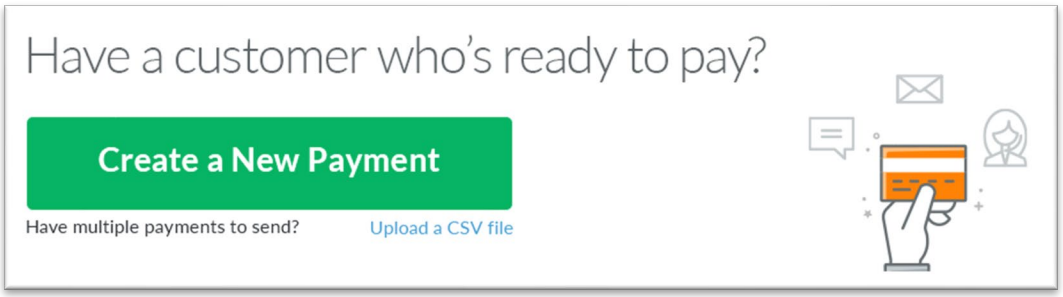
General

PayByLink in Insights supports batch creation of multiple requests using the Insights customer portal.

Work Flow Using a CSV file

To generate multiple payment-link requests using Insights:

1. Create a CSV file according to the explanations in *CSV File Format*.
2. Upload the CSV file by accessing the PayByLink page in Insights and selecting **Upload a CSV file**.



3. PayByLink validates that all the rows are formatted correctly.
4. You are prompted to enter a notification email address. Enter the email address and, click **Send**.
   *The notification helps you make sure that the request has been received and that the links have either been sent to the shoppers or are ready for you to send them.
5. PayByLink generates all the payment links and sends each as specified: to the cardholder via an email, or to the cardholder via an SMS, or only to you for further action.
6. You receive a confirmation message to the notification email address you inserted, indicating whether links were sent or only generated for you. For the generated links, a follow-up email is sent to you, containing a CSV with the links.

Note:

1. The minimum number of rows allowed in the CSV file is header + 1, and the maximum is 500.
2. The payment links will not be sent before all rows in the CSV are validated.
3. In case of an error in validation, no payment link is sent. Instead, a link appears for downloading an error report. The error report consists of the original CSV with indications of each specific error.

CSV File Format

The CSV file should be in the following format, where each field name= column name. The CSV file can contain up to 500 entries. Field names should be all lower case, as shown in the table below.

Field	Type	Min	Max	m/o/c	Description
recipient name	A-Za-z0-9	16	32	m	The name of the recipient of the message
method	[EMAIL, SMS, LINK_ONLY]	3	9	m	The method to use for sending the link: • EMAIL – Send an email to the email address listed in the **contact** field • SMS – Send a text message to the phone number listed in the **contact** field • LINK_ONLY – send a CSV file listing all generated links, to the merchant's notification email
contact	A-Za-z0-9,@,-	3	128	c (m for method=EMAIL/SMS)	The email address / phone number that will receive the payment request
amount	[0-9]	2	12	m	The requested billing amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no decimal places should be formatted according to their currency requirements. For example, a value of 1000 should be transmitted for an amount of 10.00 GBP (because the British pound has two decimal places) and a value of 10 should be transmitted for an amount of 10 JPY (because the Japanese Yen has zero decimal places). Refer to *Appendix H: Transaction Currencies* in the *Shift4 Payment API* for further information. The minimum transaction value should be 0.01 EUR (or the equivalent of EUR 0.01 in another currency), otherwise the request is rejected.

Field	Type	Min	Max	m/o/c	Description
currency	[A-Z]	3	3	m	The currency to be used in the transaction, in *ISO 4217-alpha-3* format. Every specified currency must be pre-configured on the Shift4 platform. For the supported Shift4 currency list, please refer to *Appendix F: Transaction currencies* in the *Shift4 Gateway Payment API* document.
description	A-Za-z0-9	3	128	o	Description of the purchase
invoice id	A-Za-z0-9	4	64	o	The purchase's Invoice Number
merchant reference number	A-Za-z0-9	4	64	o	Merchant reference number This optional field is a secondary transaction reference number
link_id	^[-0-9A-Za-z]+$	3	32	c (m for method=LINK_ONLY)	A reference number the merchant can use to differentiate between generated links
request id	^[-0-9A-Za-z]+$	3	32	o	The merchant's unique Request ID
representative name	A-Za-z0-9	3	32	o	The Name of the sender on behalf of the merchant
payment page language	A-Za-z0-9	2	2	o	The language in which to display the payment page. This can be used to display the payment page in the user's native language. There are several supported languages, depending on the payment page chosen skin. Refer to *Appendix E: Supported Languages* in the *Form Payment Page Specifications* for further information
notification address	URL	0	256	o	The address that will receive the payment notification once the card holder completes the payment

Note: In order to initiate a 3D secure transaction (SCA) within the CSV file you should send additional fields. Just add them as additional columns (field name = column name). For more details see *Appendix C: 3D secure*.

Batch Request using PayByLink API

General

With this API you can create a single link request or multiple requests. Each call can consist of up to 500 link requests.

Work Flow Using the API

To generate multiple payment-link requests using an API:

1. Send a payment-link API request to PayByLink.
2. PayByLink validates, online, that the request syntax is correct.
3. A synchronised response to the request is sent to you. In parallel PayByLink generates the payment links, and sends each link to the corresponding shopper via the selected method (email/sms).
4. After all the payment links are sent, a notification is sent to your server side system. The notification is mainly for you to make sure that the request has been received and that the links are now generated and have been sent to the shoppers.
5. After each successful payment, a notification is sent to your server side. This notification is optional.

Request Format

Headers

Content-Type: application/json

Authentication: Bearer {calculated string}

Body

Root-Level Fields

Field Name	m/o	Type	Min	Max	Description
request_id	m	^[-0-9A-Za-z]+$	16	32	Merchant-generated unique Request ID for the entire batch request

Object Name: merchant_info

Field Name	m/o	Type	Min	Max	Description
gw_mid	m	^[0-9A-Za-z]+$	3	8	Your assigned Gateway MID (Merchant ID)
merchant_name	m	^[0-9A-Za-z]+$	0	32	Your commercial entity name as registered with Shift4
descriptor	o	[a-zA-Z0-9]	0	22	Relevant only for a merchant who is allowed to use a dynamic descriptor. A Billing Descriptor is the descriptor that appears on the cardholder's statement in the following format: "merchant DBA Name" + "*" + "City/Customer support number", where: 1) "Merchant DBA Name" is up to 22 characters; 2) "*" is an asterisk; 3) "City/Customer support number" is up to 13 characters and is a description of the product, service or other descriptive information. We recommend listing the support phone number. Note: 1) and 3) should not include asterisks. All three parts are mandatory. If the billing descriptor does not comply with the requirements listed above, the transaction will be rejected by the gateway. For a Dynamic descriptor: • The merchant should be configured for a dynamic descriptor. • Only the 'city' part (part 3) can be overridden with dynamic content. • If the merchant is not configured for a dynamic descriptor, and the value provided in the 'city' part does not match the static descriptor – the transaction is rejected. Note: The 'merchant DBA name' that is sent to the card schemes is based on the name configured in Shift4's systems.

Field Name	m/o	Type	Min	Max	Description
notify_url	m	^.*$	0	256	The Notification Address that will receive: Notification regarding the payment links that were sent Payment notification after a shopper completes payment (if the Payment Notification option is enabled, as described in *Payment Notification*)

Object Name: batch_properties

Field Name	m/o	Type	Min	Max	Description
skin_id	o	^[0-9]+$	3	8	The selected skin of the payment page to be presented. Unique per merchant.
email_template_id	o	[0-9]	1	2	The ID of the template of the thank you email. See *"Thank you" message*.
sms_template_id	o	[0-9]	1	2	The ID of the template of the thank you text message. See *"Thank you" message*.

list Name: payment_link (constructed from the following parameters' objects)

Field Name	m/c/o	Type	Min	Max	Description
method	m	SMS|EMAIL|LINK_ONLY	3	5	The method to use for sending the link
contact	c (m for method=EMAIL/SMS)	^[+]+[-() 0-9]+|[^]+@[^]+\\.[^]+$	4	128	The email address / phone number that will receive the payment request
link_id	c (m for method=LINK_ONLY)	^[-0-9A-Za-z]+$	3	32	A reference number the merchant can use to differentiate between generated links
request_id	o	^[-0-9A-Za-z]+$	16	32	Merchant-generated unique Request ID for this specific payment request

Field Name	m/c/o	Type	Min	Max	Description
merchant_reference_number	o	^[-0-9A-Za-z]+$	0	32	This optional field is a secondary Transaction Reference Number which can be transmitted alongside the Transaction Reference Number transmitted via the a1 parameter. Note: No plaintext cardholder data should be provided in this field.
representative_name	o	^[-0-9A-Za-z]+$	3	32	The name of the sender on behalf of the merchant
email_template_id	o	[0-9]	1	3	The ID of the template of the thank you email. See *"Thank you" message*. With this value, you can differentiate between this specific request and other requests.
sms_template_id	o	[0-9]	1	3	The ID of the template of the thank you text message. See *"Thank you" message*. With this value you can differentiate between this specific request and other requests.
skin_id	o	[0-9]	1	3	The selected skin of the payment page to be presented. Can change from request to request. With this value you can differentiate between this specific request and other requests.
payment_page_language	o	[A-Z]	2	2	The language in which to display the payment page. This can be used to display the payment page in the user's native language. The supported languages include: EN, CN, DE, ES, FR and RU.

Field Name	m/c/o	Type	Min	Max	Description
Note:	You can add any parameter found in *Shift4 Payment API* documentation under this root. For example, parameters j1-j4-				

```
"payment_link": [
    {
      "purchase_info": {
        "invoice_number": "111333"
      },
      "method": "LINK_ONLY",
      "amount": {
        "amount": "120",
        "currency": "USD"
      },
      "link_id": "123456",
      "request_id": "1111111111111111",
      "j1": "19901215",
      "j2": "560070",
      "j3": "CR0 2GF",
      "j4": "Gooden",
    }
]
```

Object Name: amount

Field Name	m/o	Type	Min	Max	Description
amount	m	[a-zA-Z0-9]	1	10	The requested billing amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no decimal places should be formatted according to their currency requirements. For example, a value of 1000 should be transmitted for an amount of 10.00 GBP (because the British pound has two decimal places) and a value of 10 should be transmitted for an amount of 10 JPY (because the Japanese Yen has zero decimal places). Refer to *Appendix H: Transaction Currencies* in the *Shift4 Payment API* for further information. The minimum transaction value should be 0.01 EUR (or the equivalent of EUR 0.01 in another currency), otherwise the request is rejected.
currency	m	[A-Z]	3	3	The currency to be used in the transaction, in *ISO 4217-alpha-3* format. Every specified currency must be pre-configured on the Shift4 platform. For the supported Shift4 currency list, please refer to *Appendix F: Transaction currencies* in the *Shift4 Gateway Payment API* document.

Object Name: purchase_info

Field Name	m/o	Type	Min	Max	Description
description	o	[a-zA-Z0-9]	0	127	Description of the purchase
invoice_number	o	[a-zA-Z0-9]	0	127	Purchase Invoice Number

Object Name: shopper_info

Field Name	m/o	Type	Min	Max	Description
last_name	m	[a-zA-Z0-9]	3	32	The shopper's last name. If shorter than three characters, you must add additional characters
first_name	m	[a-zA-Z0-9]	3	32	The shopper's first name. If shorter than three characters, you must add additional characters

Note

1. Using the API requires IP whitelisting (see *Security of the Payment Notification*).
2. The minimum number of requests in a single API call = 1, the maximum = 500.
3. Shift4's Smart 3D Secure can be added to the API call by adding the relevant parameters (see *Appendix C: 3D secure*).

Examples

The following are examples of an API request sent to PayByLink with a batch request for multiple payment links, and the response to the batch request for multiple payment links.

Batch Request Example

```
{
  "merchant_info": {
    "gw_mid": "10000330",
    "merchant_name": "Baseball",
    "notify_url": "https://enogr5okg6tgk.x.pipedream.net"
  },
  "request_id": "1111111111111111",
  "batch_properties": {
    "skin_id": "35",
    "email_template_id": "4",
    "sms_template_id": "1"
  },
  "payment_link": [
    {
      "purchase_info": {
        "invoice_number": "111333"
      },
      "method": "LINK_ONLY",
      "amount": {
        "amount": "120",
        "currency": "USD"
      },
      "link_id": "123456",
      "request_id": "11111111111111111"
```

```
    },
    {
      "shopper_info": {
        "first_name": "Claudet",
        "last_name": "Lavigne",
        "email": "claudet.lavigne@geludkita.tk"
      },
      "redirect_urls": {
        "success_url":
"https://www.clker.com/cliparts/K/m/g/9/O/v/check-mark-md.png",
        "fail_url": "https://vignette.wikia.nocookie.net/universal-
crusade/images/a/a5/X.png/revision/latest?cb=20170903062123"
      },
      "purchase_info": {
        "invoice_number": "111335"
      },
      "representative_name": "Jorden Carol",
      "method": "EMAIL",
      "contact": "claudet.lavigne@geludkita.tk",
      "amount": {
        "amount": "120",
        "currency": "USD"
      },
      "merchant_reference_number": "1113",
      "request_id": "11111111111111113",
      "payment_page_language": "fr"
    }
  ]
}
```


Batch notification example

The following is an example of a response to a batch request, notifying you which payment links were successfully sent to shoppers.

```
{
   "batch_id":"5b56d667b97d4be89f4c277cf637bb36",
   "datetime_received":"27/05/2019 12:35:15",
   "datetime_end_processing":"27/05/2019 12:35:24",
   "payment_link":[
      {
         "request_id":"1111",
         "amount":{
            "amount":"10",
            "currency":"USD"
         },
         "method":"EMAIL",
         "result":{
            "response_code":"000",
            "response_description":" Request has been executed
successfully"
         }
      },
      {
         "request_id":"4444",
         "amount":{
            "amount":"25",
            "currency":"EUR"
         },
         "method":"EMAIL",
         "result":{
            "response_code":"000",
            "response_description":" Request has been executed
successfully"
         }
      }
   ]
}
```


Batch Response Example


```
{
    "batch_id": "c3ae5f3022024291b3644eca19d66955",
    "result": {
        "response_code": "000",
        "response_description": "Batch Request Received. processing
request."
    },
    "payment_link": [
        {
            "request_id": "11111111111111111",
            "merchant_info": {
                "gw_mid": "10000330",
                "merchant_name": "Baseball"
            },
```

```
            "shopper_info": {
                "email": "claudet.lavigne@geludkita.tk",
                "first_name": "Claudet",
                "last_name": "Lavigne"
            },
            "amount": {
                "amount": "120",
                "currency": "USD"
            },
            "purchase_info": {
                "description": "description Name order",
                "invoice_number": "111333",
                "digital_goods": false,
                "one_click": false,
                "mobile_view": false
            },
            "redirect_urls": {
                "success_url":
"https://www.clker.com/cliparts/K/m/g/9/O/v/check-mark-md.png",
                "fail_url":
"https://vignette.wikia.nocookie.net/universal-
crusade/images/a/a5/X.png/revision/latest?cb=20170903062123",
                "cancel_url": null,
                "pending_url": null
            },
            "create_token": false,
            "method": "EMAIL",
            "contact": "claudet.lavigne@geludkita.tk",
            "skin_id": "35",
            "merchant_reference_number": "1113",
            "representative_name": "Jorden Carol",
            "payment_page_language": "fr"
        }
    ]
}
```


"Thank you" message

PayByLink offers the option of sending a message (via email/text, depending on how the link was sent) to the shopper after payment is successfully completed.

For example:

“Dear {{customer name}},

Your payment to {{merchant name}} was received successfully.

As always, our 24/7 Support team is available to assist you with any question.

Best regards,

{{merchant name}}”

Note: To implement a thank you message, please contact your solution architect.

GET (Retrieval) Request

Get Batch Status

After sending all the requested payment links, PayByLink returns a batch_id to you. This value can be used in order to query for the status of the corresponding payments. If the GET is received when not all payment links were sent, no result is returned.

Request structure:

```
url: https:// sourcepayments.com/payments/rest/payment_link/{gw_mid}/batch/{request_id}
```

Get Single Request Status

You can also query for a specific payment link status, using the specific request_id.

Request structure:

```
url: https:// sourcepayments.com/payments/rest/payment_link/{gw_mid}/{request_id}
```

The GET request should be formatted without a “Body” to the transaction retrieval request. Furthermore, the request headers are identical to the original request’s headers.

Example

Headers:

Authentication: Bearer S8LdnyW+9y1fffhr9w8rA6lCmbU9m9/eS88cYhtFjX9UA19FQEA+LQ02waVsywg2BBnWvOxATBF14NvKxwXF6w==

Payment Notification (Recommended)

The notification service is recommended for better control of the transaction flow through the PayByLink Payment Page; it is applicable to all transactions. The notification service sends you the result of the processed transaction on a secure channel, before the shopper is redirected to the Success/Fail page. You must send a response back to Shift4 upon receiving the notification. If a response is not received, Shift4 instantly cancels the transaction and the shopper is redirected to the default 'Fail URL'.

Enabling this notification provides you with assurance that the shopper has completed payment for the transaction. The option of enabling notifications is part of the onboarding process.

Payment Notification Response

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

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

Security of the Payment Notification

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

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

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

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

Appendix A: SHA512 Transaction Signature

Every Shift4 PayByLink 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" : "Aa123456"
},
"amount" : {
"amount" : "5000",
"currency" : "EUR"
}
}
```

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

ab0d5e7e06c0d8ee9358f1fe2c2728cc76b24e3b4b9a3de4ec6e45693b290ce27a750feaec76469e7bc309bc680700e6f79217b73e6aa3dcda19d9f7fd5fcf31

Appendix B: Response Codes

For the full list of 'initiate payment request' response codes and their description, please refer to *Appendix B: Operation Result Codes* in the *Shift4 Payment Gateway API* document. This appendix lists the most common response codes.

z2 (Response code)	z3 (Description)
-63	The requested gateway MID is not enrolled in the 3D-secure service
-50	An error occurred during the 3D secure process
-38	The transaction has been denied by the Gateway because 3D secure Authentication failed
-36	The selected Processor does not support some of the transaction's parameters
-35	The selected MID is not registered to your account
-33	You need to be registered with the routing service to complete the routing request
-32	You are not registered with the selected Processor
-31	Authentication process aborted by cardholder
-30	Transaction Failed due to error in 3D secure process
-13	The requested gateway MID is not enrolled in the 3D Secure Adviser service
-10	Internal server error. Please contact Shift4 support.
-9	Parameter is malformed: [Field]
-7	Incorrect response from the gate. Connection is broken.
0	Request has been executed successfully
21	Merchant not found, or K is not valid
22	PKey has expired or cannot be found
23	Parameter is missing: [Field]
24	The authentication process failed
25	Transaction has been denied, please try again
26	Transaction declined. There was a problem in the 3D-secure process
32	Notification timeout, Transaction has failed

Appendix C: 3D secure

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

Shift4 Payment Gateway offers two modules of 3D Secure:

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

Note:

1. Shift4's 3D Secure service supports both versions of the 3D Secure protocol: 3D Secure 1.0 and 3D Secure 2.0
2. To use Shift4's 3D Secure service, you must be registered to the service and have it activated on your account.

Contact your account manager for more information.

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

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

In some cases, the issuer may still want to perform more extensive checks and require the cardholder to respond to a 'challenge'. The challenge can be one or more of the following: entering a one-time-password or other credentials, answering a secret question and/or identifying yourself using a biometric based device (fingerprints, face recognition, etc.). Issuers that are still using the old 3D Secure 1.0 protocol require the cardholder to respond to a challenge for every 3D secure transaction. The Shift4 Payment Gateway 3D Secure service automatically selects the correct 3D Secure flow based on the 3D secure protocol supported by the Issuer.

Initiating the 3D Secure process

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

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

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

Note:

- The transaction will only be processed if the 3D Secure process is completed successfully, whether in a frictionless flow or a challenge flow
- When initiating Smart3DSecure, if the decision engine determines the transaction should go through the 3D Secure process it can go through any of the standard 3D secure flows
- You can also choose to only go through the 3D Secure authentication process without actually processing the transaction. To do so use operation code [98] (for further details see the *Shift4 Payment Gateway API* document).

3DS Adviser

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

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

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 that a specific transaction be exempt from the SCA process, based on the transaction characteristics.

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

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

Additional Response parameters for the 3DS Adviser Module

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

Name	Type	Min	Max	Description
smart_3ds_result	[0-2]	2	2	Describes the 3DS Adviser module recommendation: 01: Do 3D secure 02: Skip 3D secure
smart_3ds_result_reason	[a-zA-Z0-9]	0	128	Includes the rule ID which was executed as part of the Smart 3D rule engine

Additional Parameters for Improved 3D Secure Assessment

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

Recommended Parameters

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

Requested Data	Shift4 Parameters	Description
Brower IP address	d1	IP address of the browser as returned by the HTTP headers. In either ipv4 or ipv6 format
Buyer email address	c3	Cardholder's email address in valid email address format, such as *joe@bloggs.com*
Billing Information	c4	Cardholder Billing Address street number
	c5	Cardholder Billing Address street name
	c7	Cardholder Billing Address city name
	c8	Cardholder Billing Address Territory Code, a level 2 country subdivision code according to ISO-3166-2. A reference list can be found at *ISO 3166-1-alpha-2*.
	c9	Cardholder Billing Address Country Code. Please refer to *ISO 3166-1-alpha-2* for a list
	c10	Cardholder Billing Address Postal/ZIP Code
Shipping information	3ds_shipaddrcity	City of the shipping address requested by the Cardholder

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

Request parameters

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

Name	Description	Type	min	max	m/o/c
3ds_channel	Indicates the type of channel interface being used to initiate the transaction. The accepted values are: 01 - App-based (APP) 02 - Browser (BRW) 03 - 3DS Requestor Initiated (3RI)	[0-3]	2	2	o
3ds_redirect_url	Contains the merchant URL to which the browser should be redirected after the challenge session	[a-zA-Z0-9]	0	2048	m
3ds_category	Identifies the category of the message for a specific use case. The accepted values are: 01 - PA (Payment authentication) 02 - NPA (Non-payment authentication) 80 – Data only (Mastercard only, valid only for 3ds_channel = 01 or 02)	[0-3]	2	2	o

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

Name	Description	Type	min	max	m/o/c
3ds_reqchallengeind	Indicates whether a challenge is requested for this transaction. For example: For *3ds_category* 01 (PA), a merchant may have concerns about the transaction, and request a challenge. For *3ds_category* 02 (NPA), a challenge may be necessary when adding a new card to a wallet. 01 - No preference 02 - No challenge 03 – Optional challenge 04 – Mandatory challenge 05 - No Challenge Requested, transactional risk analysis is already performed 06 - No Challenge Requested, Data share only 07 - No Challenge Requested, SCA is already performed 08 - No challenge requested (utilise whitelist exemption if no challenge required) 09 - Challenge requested (whitelist prompt requested if challenge required)	[0-4]	2	2	o
3ds_reqpriorref	This data element provides additional information to the issuer to determine the best approach for handling a request. The element contains the issuer's Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the cardholder).	[a-zA-Z0-9]	0	36	o
3ds_reqpriorauthmethod	Mechanism that was used by the cardholder to previously authenticate to the merchant. Accepted values for this field are: 01- Frictionless authentication performed by the issuer 02 - Cardholder challenged by the issuer 03 - AVS verified 04 - Other issuer methods	[0-4]	2	2	o
3ds_reqpriorauthtimestamp	Date and time in UTC of the prior authentication. Accepted date format is YYYYMMDDHHMM.	[0-9]	12	12	0

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

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

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

Name	Description	Type	min	max	m/o/c
3ds_addrmatch	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical. Accepted values: • true - Shipping Address matches Billing Address • false - Shipping Address does not match Billing Address Note: the default value of this field is 'false'	[a-z]	4	5	o
c2	Cardholder's contact phone number	[0-9\-\.]	5	32	o
c3	Cardholder's email address This parameter should be transmitted as a valid email address such as *joe@bloggs.com* A default valid email address should always be transmitted in Card-Present transactions.	email	7	64	o m – when initiating 3D secure transaction
c4	Cardholder Billing Address street number If the processor supports AVS then the transmission of this parameter will activate the AVS system. Note that the street number should be omitted from the c5 parameter if a c4 parameter is transmitted.	[0-9]	1	16	o m – when initiating 3D secure transaction
c5	Cardholder Billing Address street name Note that the street number should not be included here if the c4 parameter is being transmitted.	[a-zA-Z0-9\ \-]	4	50	o m – when initiating 3D secure transaction
c7	Cardholder Billing Address city name	[a-zA-Z\ \-]	3	30	o m – when initiating 3D secure transaction

Name	Description	Type	min	max	m/o/c
c8	Cardholder Billing Address Territory Code, a level 2 country subdivision code according to ISO-3166-2. A reference list can be found at *ISO 3166-1-alpha-2.*	[a-zA-Z0-9]	1	3	o m – when initiating 3D secure transaction
c9	Cardholder Billing Address Country Code Please refer to *ISO 3166-1-alpha-2* for a list.	[A-Z]	2	2	o m – when initiating 3D secure transaction
c10	Cardholder Billing Address Postal/ZIP Code If transmitted, this value is sent to the issuer and forms part of their AVS checks (not all payment processors support AVS checks. Please refer to the *Shift4 Payment Gateway: Processors Specification* for further details).	[a-zA-Z0-9\ \-]	1	9	c m – when initiating 3D secure transaction
3ds_homephonecountry	Country Code of the home phone.	[0-9]	1	3	o
3ds_chmobilephone	The mobile phone provided by the cardholder, without the country code	[0-9]	0	18	o
3ds_mobilephonecountry	Country Code of the mobile phone.	[0-9]	1	3	o
3ds_chworkphone	The work phone provided by the cardholder, without the country code	[0-9]	0	18	o
3ds_workphonecountry	Country Code of the work phone.	[0-9]	1	3	o
3ds_shipaddrcity	City of the shipping address requested by the cardholder.	[a-zA-Z]	3	32	o

Name	Description	Type	min	max	m/o/c
3ds_shipaddrcountry	Country of the shipping address requested by the cardholder. Refer to *ISO 3166-1-alpha-2* for a list.	[A-Z]	2	2	c m – if 3ds_shipaddrstate exists or if shipping information is not the same as billing information
3ds_shipaddrline1	First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.	[a-zA-Z]	0	128	o m – when 3ds_addrmatch = false
3ds_shipaddrline2	Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.	[a-zA-Z]	0	128	o m – when 3ds_addrmatch = false
3ds_shipaddrpostcode	ZIP or other postal code of the shipping address associated with the card used for this purchase.	[a-z0-9]	0	16	o m – when 3ds_addrmatch = false
3ds_shipaddrstate	The state or province of the shipping address associated with the card used for this purchase. The value should be the country subdivision code defined in ISO 3166-2.	[0-9]	3	3	o m – when 3ds_addrmatch = false

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

Name	Description	Type	min	max	m/o/c
3ds_reorderitemsind	Indicates whether the cardholder is reordering previously purchased merchandise. Accepted values are: 01 - First time ordered 02 - Reordered	[0-2]	2	2	o
3ds_preorderpurchseind	Indicates whether the cardholder is placing an order for merchandise with a future availability or release date. Accepted values are: 01 - Merchandise available 02 - Future availability	[0-2]	2	2	o
3ds_preorderdate	For a pre-ordered purchase, the expected date when the merchandise will be available. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_giftcardamount	For prepaid or gift card purchase, the purchase amount total of prepaid or gift card(s) in major units (for example, USD 123.45 is 123).	[0-9]	1	12	o
3ds_giftcardcurr	For prepaid or gift card purchase, the currency code of the card as defined in *ISO 4217-alpha-3*, except for codes 955 - 964 and 999.	[0-9]	3	3	o
3ds_giftcardcount	For prepaid or gift card purchase, the total count of the individual prepaid or gift cards/codes purchased. Field is limited to 2 characters.	[0-9]	0	2	o
3ds_purchasedate	Date and time of the purchase expressed in UTC. The field is limited to 14 characters, formatted as YYYYMMDDHHMMSS.	[0-9]	14	14	m
3ds_recurringexpiry	Date after which no further authorisations will be performed. This field is limited to 8 characters, and the accepted format is YYYYMMDD. This field is required if *3ds_reqchallengeind* = 02 or 03.	[0-9]	8	8	c
3ds_recurringfrequency	Indicates the minimum number of days between authorisations. The field is limited to a maximum of 4 characters. This field is required if *3ds_reqchallengeind* = 02 or 03.	[0-4]	0	4	c

Name	Description	Type	min	max	m/o/c
3ds_transtype	Identifies the type of transaction being authenticated. The values are derived from ISO 8583. Accepted values are: 01 - Goods / Service purchase 03 - Check Acceptance 10 - Account Funding 11 - Quasi-Cash Transaction 28 - Prepaid activation and Loan	[0-9]	2	2	o
3ds_merchantname	Assigned merchant name	[a-zA-Z0-9]	0	32	o

Response parameters

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

Change History

Version	Subject/Date	Description
2.2	November 2023	Rebrand to Shift4
2.1	March 2023	Added note in payment_link root regarding the option to add any Shift4 API parameter under this root
2.0	January 2021	Addition of new link only functionality and description Addition of 3DS 2.2-related Decoupled Authentication, Whitelisting and Authentication fields and settings Updated API format with new parameters and updated API call examples
1.0 rev 1	July 2020	Updated the Smart 3D Secure chapter Updated the notification IPs' range
1.0	October 2019	First Release

Support Information

EU: +356.2778.0876

UK: +44.20.3608.1288

US: +1.617.715.1977

Email: support.europe@shift4.com