SHIFT4™

API Specifications

Payments Gateway

Version 1.9 rev 6 | May 2024

Contents

Introduction

The purpose of this document is to provide an in-depth description of the *Shift4* Payment Gateway API, a proprietary platform for Payment Gateway services.

The *Shift4* API is connected to various Payment Processors around the world. You must be registered with at least one Payment Processor in order to accept payments.

The *Shift4* API employs a basic 'request-response' model where the Merchant instructs the gateway to perform an operation and the gateway responds with that operation's status.

It also employs a simple-to-use name/value pair data format based on HTML form-urlencoded data.

This document describes the Payment Gateway processing features supported by the *Shift4* API. Note, however, that processors may differ in their support of these operations and features, and some may not be available when used with a specific processor.

Glossary

Term	Description
Payment Gateway	A Payment Gateway is an application for authorising payment transactions such as those made with debit and credit cards, or with alternative payment methods. It is designed for both online and physical businesses. A Payment Gateway facilitates a payment transaction by transferring information between a merchant portal (such as a website, a point-of-sale device (POS), a mobile phone application or Interactive Voice Response (IVR) service) and the Payment Processor or acquiring bank.
Payment Processor	A Payment Processor is a payment service provider appointed by the merchant (often as a third party) to process transactions from various channels via one or more acquiring banks.
Authorisation	An Authorisation (Auth) request is initiated by the merchant portal and sent to the Gateway in order to verify that sufficient funds are available and reserved for settling the payment transaction in due time. If the Authorisation is approved, the issuer bank returns an Authorisation code and the amount of funds authorised. Note that no actual funds are collected during an Authorisation request.

Term	Description
Capture	A Capture request instructs the issuer to transfer funds from the cardholder's bank account to the merchant's bank account. This transaction can only be performed after an Auth transaction.
Sale	A Sale request instructs the Gateway to perform both Authorisation and Capture transactions at the same time, i.e., to send an Authorisation request to the issuer and immediately capture the transaction upon its approval.
Void	A Void request is a merchant-initiated request that instructs the Gateway to cancel a transaction. In case of auth void the action also releases the reserved funds from the cardholder account.
Credit	There are two types of Credit requests: (1) Referral Credit, a request that instructs the Gateway to refund a previously captured transaction to the cardholder, and (2) Independent Credit, a request that initiates a stand-alone credit transaction. Full card number is needed.
CFT	A CFT (Credit Fund Transfer) request is a merchant-initiated request that instructs the Gateway to transfer funds to the cardholder's account. This transaction is allowed for specific Merchant Category Codes (MCCs).
AVS	The Address Verification System (AVS) is a security measure for verifying the address of a person claiming to own a credit card.
Token Transactions	Token Transactions (also known as Card-on-File transactions) store the cardholder's card data during the first purchase and reuse this data for subsequent purchases without requiring the cardholder to re-enter her/his card details.
ZIP+4	An expanded ZIP code system used by the U.S. Postal Service that uses the basic five-digit code plus four additional digits.

Term	Description
Billing Descriptor	A Billing Descriptor appears on the cardholder's statement and contains the name of the business (frequently referred to as "Doing Business As" or DBA) and the relevant transaction information (such as the merchant's location or product name). The Billing Descriptor allows the cardholder to identify the specific purchases associated with the transactions recorded on their statement. The *Shift4* system supports two types of Billing Descriptors: • A Static Billing Descriptor defined once by the merchant and subsequently used for all transactions • A Dynamic Billing Descriptor that allows the merchant to change the information included in each transaction. Note: Providing clear billing descriptors can help the cardholder to recognise the transaction and reduce chargebacks and disputes.

Useful Documents / References

The following documents may also be useful in understanding the Shift4 Payment Gateway API Specification:

- Shift4 Card-Present Specification – a supplement to the *Shift4 Gateway API Specification* that provides detailed information on the API's use of Card-Present data.
- *Shift4 Processors documentation* - select the specification for the processor you work with, can be found on the Shift4 Developers Portal.

Certification

All new implementations must complete a certification process before they can start sending production transactions, in order to ensure the quality of integration and integrity of merchant data.

Please note that only test-card data should be used for testing.

Additional certifications are required if the implementation makes use of new operation codes or features.

Please contact integration.europe@shift4.com for latest test card details and more information

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 earlier versions of the API specification.

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

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

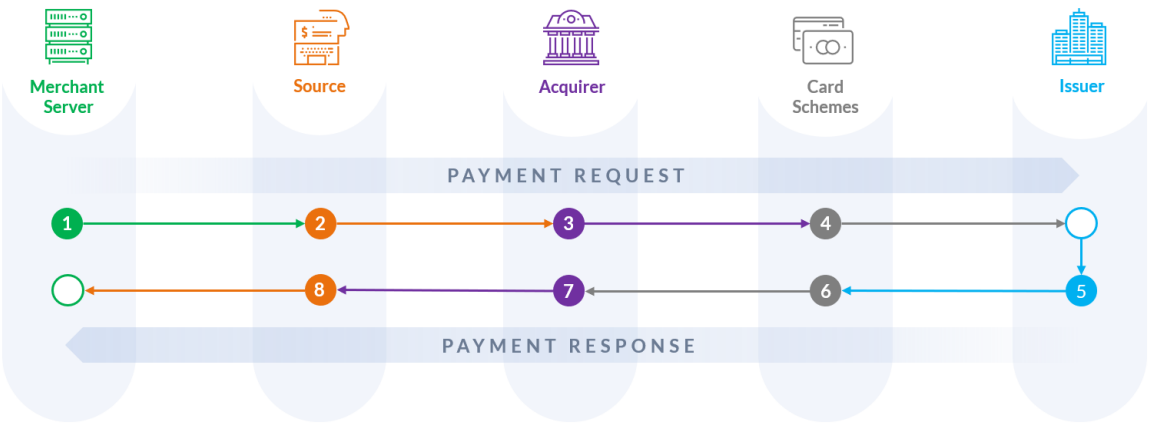
Publisher Information

Gateway Interface

Introduction

Transaction requests are sent online and in real-time using the HTTPS (Hypertext Transfer Protocol - Secure) protocol. In addition, the Gateway protocol exposes multiple operation types.

Note that *Shift4* is connected to multiple Payment Processors that may differ in the way they support various operations and features. A payment flow is a synchronised request-response flow as described in the following diagram. However, there are cases in which more than one request-response flow is required, and cases that involve other entities such as the cardholder browser (for example, 3D secure flows described in Appendix I: 3D Secure).



Uniform Resource Locators (URLs)

Integration URL	https://intconsole.credorax.com/intenv/service/gateway
Production URL	https://xts.gate.credorax.net/crax_gate/service/gateway

HTTP Specification

- Protocol: HTTPS
- Supported charset: UTF-8
- Method: POST
- Content-Type: [application/www-form-urlencoded] or [application/x-www-form-urlencoded]

Example HTTP Request

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

Host: intconsole.credorax.com

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

Content-Length: 176

M=8632876&K=9823ou1pwieufdp91873p98723rp987238r97p198r&O=1&a1=7894654&a4=1099&b1=45454545454054545&b2=1&b3=08&
b4=11&b5=003&c1=John+Smith&c3=johnsmith@yahoo.com&d1=111.222.0.101

Note:

- Please honor a TTL of at least 30 seconds for each single session per HTTPS request.
- Each processor may have a different TTL. Refer to the Shift4 Global Processors Specifications document for further information.

Security/Authentication

All HTTP requests must be sent through a secure channel and over SSL (Secure Sockets Layer). The Shift4 Payment Gateway employs a non-authenticated SSL session and does not authenticate the SSL session by examining a client certificate. Instead, the client is first authenticated by its source IP and by a secondary authentication check that employs a SHA256 message cipher sent in the request payload. This SHA256 message cipher, in turn, can be verified by the merchant before ending the transaction's processing. See Appendix A: Message Cipher for further details.

Health Checks

You can check the health of the *Shift4* Payment Gateway and Integration Environments by accessing the following URLs:

Integration URL	https://intconsole.credorax.com/intenv/service/status
Production URL	https://xts.gate.credorax.net/brain/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":false

The following recommendations should be followed when using this service:

- A maximum of **one** health check is permitted every 10 seconds

If no response is received within 20 seconds the health check request should be considered timed-out

- Consider our processing service unavailable after 3 consecutive service failures of the health check

Please contact the Shift4 Support Team immediately in the event of any unexpected service interruption, at: support.europe@shift4.com

or at our 24/7 telephone numbers EU +356 2778 0115 | UK +44 20 3608 1288 | US +1 617 715 1977

Gateway Features

The Shift4 Payment Gateway API offers the following services and functionalities. Note that some services require prior registration.

Address Verification System (AVS)

The Address Verification System (AVS) is a security measure that compares the cardholder-provided Billing Address with the Cardholder Address recorded by the issuer bank.

This security measure may help in reducing fraud and chargebacks in card-not-present transactions.

It should be noted that the AVS check is carried out by the issuer bank (and not by *Shift4*) through an examination of the values transmitted in the c4, c5 and c10 parameters.

Note:

- AVS data is optional for all clients
- AVS is supported by issuers mainly in the United States, Canada and the UK.

Card-Present

Card-Present service allows you to accept payment using a variety of POS (point-of-sale) devices. For more information, please refer to the Shift4 Card-Present Specification document.

Card Validation

Card Validation, also known as Zero-Value Authorisation, is an account status inquiry sent to the cardholder's issuer bank by using the a9 parameter.

CVV/CVV2/CVC2

CVV is the security number (3 or 4 digits) usually displayed on the back of the payment card. A valid CVV value is required for all card transactions apart from the following cases:

- Card-Present transactions (a2=6, 8, 10)
- Subsequent recurring transactions (a9=2)
- Mail Orders (a2=4)

CVV checks are operated as part of operation codes [1], [2], [23], [10], [28] and are transmitted by using the b5 parameter.

If you want to verify whether a CVV is required on your transactions, contact your account manager for further explanation.

Dynamic Descriptor

The Dynamic Descriptor functionality allows the merchant to have a different descriptor displayed on the cardholder's card statement with every transaction. This functionality requires your selected Payment Processor's approval before using it. See more details in the description of the i2 parameter.

Note:

The Dynamic Descriptor can only be used in card-not-present transactions.

SmartGuard

SmartGuard is an anti-fraud protection service that protects your revenue by assessing fraud activity in real time. Powered by Machine Learning technology and fraud rule engine capabilities, the SmartGuard service accurately identifies fraudulent payments, so that you can accept more legitimate payments and reduce your false-positive rate. The SmartGuard service offers an automatic solution using Machine Learning technology, and the ability to control and manage your anti-fraud protection settings based on data-driven decisions.

For more information, please refer to the SmartGuard parameters.

Note:

The SmartGuard service requires prior registration. Contact your Shift4 account manager for more details.

Smart Routing

Smart Routing allows you to control and manage your transaction traffic to different Payment Processors using a flexible rule engine and ad-hoc routing capabilities. Routing your transactions to the most suitable Payment processor allows you to optimise your payments activity in various business parameters such as:

- Payments approval rate
- Payments costs
- Payments availability
- Risk management

Note:

The Smart Routing service requires prior registration. Contact your Shift4 account manager for more details.

Token Engine (Card-on-File)

The Token Engine protects sensitive card data by replacing the cardholder's Primary Account Number (PAN) with a series of randomly-generated numbers known as a *token*. Tokens can then be securely transferred via the internet or via wireless networks in order to process the cardholder's payment without exposing sensitive bank details. The bank account number itself, in turn, is placed in a secure token vault.

The Token Engine is operated with a dedicated set of operation codes that allow you to create new tokens, use existing tokens or block them from future use. Read more about this functionality in the Card-on-File section.

3D Secure

The 3D Secure service is an authentication protocol designed for creating an additional security layer for online transactions.

Shift4 Payment Gateway supports all versions of the 3D Secure protocol: 3D Secure 1.0, 2.0, 2.1.0 and 2.2.0.

The Shift4 Payment Gateway 3D secure functionality is integrated into the transaction flow and described in more details in Appendix I: SCA & 3D Secure.

You can also choose to use an external MPI or 3D Secure service provider, and provide the 3D Secure data using the i8 parameter.

Note:

For more information of the Shift4 Payments Platform products and services, contact your Shift4 account manager.

Required Fields

The *Shift4* Payment Gateway provides 4 operation groups:

- Basic operations
- Referral operations
- Token operations (Card-on-File)
- Special operations

The following tables describe the available API parameters and specify whether the field is mandatory (m), conditional (c), optional (o), or not used (-).

Note:

- The number in square brackets is a unique operation code.
- Each processor may have different required fields. Refer to the Shift4 Global Processors Specification document for further information

Basic Operations

The basic group includes three operations, for transmitting basic Authorisations, Sales and Refunds:

Basic Operations	
[1]	Sale
[2]	Authorisation
[6]	Independent Credit

[1] – Sale

A Sale consists of an Authorisation and Capture request. If the Authorisation is successful, the transaction will be automatically captured and included in the next clearing file.

[2] – Authorisation

An Authorisation generates an online authorisation request.

[6] - Independent Credit

An Independent Credit operation initiates a refund request in the next clearing file.

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
M	Shift4 assigned gateway merchant ID	[A-Z0-9_]	3,8	m

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
K	Unique cipher used for authenticating requests Refer to Appendix A: Message Cipher for further details on how to generate the cipher.	[0-9A-Za-z]	1,32	m
O	Operation Code The operation code is used for determining the requested service. See the list in Basic Operations.	[0-9]	1,3	m
a1	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. Note: No plaintext cardholder data should be provided in this field.	[A-Za-z0-9-]	1,32	m
a2	Payment source type Valid options are: 2 Online Order (default value) 3 Telephone Order 4 Mail Order 5 Virtual Terminal	[0-9]	1,2	o
a4	Requested billing amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no exponents should be formatted according to their currency requirements. Refer to Appendix H: Transaction Currencies for further information. The minimum transaction value should be 0.01 EUR (or the equivalent or EUR 0.01 in another currency), otherwise the request is rejected.	[0-9]	1,12	m

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
a5	Transaction currency Indicates the currency that should be used in the transaction (every currency used must be preconfigured on the Shift4 platform). Refer to ISO 4217-alpha-3 for further information.	[A-Z]	3,3	m
a6	Transaction date (local date of the transaction)	yyMMdd	6,6	o
a7	Transaction time (local time of the transaction)	HHmmss	6,6	o
a9	Transaction type. Valid values are: **Value** **Description** 1 First standing order 2 Subsequent standing order 5 Card-Only Validation 6 Straight Operation 8 Unscheduled Card-on-File transactions initiated by the merchant 9 Unscheduled Card-on-File transactions initiated by the cardholder 10 Card validations for an unscheduled Card-on-File 11 First Subscription 12 Subscription Note: By default, the transaction type is considered a straight operation unless specified otherwise.	[0-9]	1,2	c ([1], [2] for recurring)
a10	Authorisation Type: 1 Final Authorisation (default value) 2 Pre-Authorisation 3 Deferred Authorisation Transactions referring to Pre-Authorisations must include an a4 parameter.	[1-3]	1,1	c (mandatory for [1],[2] only)

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
a11	Multiple Capture tag Indicates the number of expected Captures Only supported in Card-not-Present transactions Default value is 1 Max value is 98 Min value is 2	[0-9]	1,2	c (mandatory for [2] only)
a14	Partial Authorisation tag This request parameter indicates to the issuer whether you are willing to accept partial authorisation approval. Possible values: 0 – Full authorisation only (default) 1 – Partial authorisation also accepted	[0,1]	1,1	c (mandatory for [2] only)
a19	Recurring payment frequency **Value** **Description** 1 Daily 2 Twice weekly 3 Weekly 4 Ten days 5 Fortnightly 6 Monthly 7 Every two months 8 Trimester 9 Quarterly 10 Twice yearly 11 Annually 12 Unscheduled (default value)	[0-9]	1,2	o
b1	PAN – Primary Account Number	[0-9]	8,19	m
b3	Card expiration month Two-digit number (*mm* format)	[0-9]	2,2	m

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
b4	Card expiration year Two-digit number (*yy* format)	[0-9]	2,2	m
b5	Card security code (CVV / CVC) as printed on the card	[0-9]	3,4	m (o for [6])
b21	Passthrough wallet indicator Indicates whether the transaction originally issued from a passthrough wallet supported by Shift4. Possible values: • applepay: for Apple Pay • googlepay: for Google Pay • samsungpay: for Samsung Pay • vts_mdes_token: for VTS and MDES for Merchants) token-based transactions	[A-Za-z\ ]	8-14	c (m if transaction was originally Apple Pay, Google Pay, Samsung Pay or a VTS/M4M transaction)
c1	Cardholder's full name The minimum length of this field is five characters. If the cardholder provides a name that is less than five characters long, you must either add additional non-space characters to the name (e.g. Mr. Lu) or not transmit the field at all	[\ a-zA-Z]	5,45	c recommended – when initiating 3D secure transaction m for Visa 3Ds transactions
c2	Cardholder's contact phone number Note: For Visa 3ds transactions cardholder's phone number or email are mandatory.	[0-9\-\.]	5,32	c m for Visa 3ds transactions, o if c3 is sent. For 3DS transactions always include 3ds_homephonecountry.

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
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. Note: For Visa 3ds transactions cardholder's phone number or email are mandatory.	email	7,64	c m – when initiating 3D secure transaction. o if c2 is sent.
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 recommended – 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 recommended – when initiating 3D secure transaction
c7	Cardholder Billing Address city name	[a-zA-Z\ \-]	3,30	o recommended – when initiating 3D secure transaction
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 recommended – when initiating 3D secure transaction

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
c9	Cardholder Billing Address Country Code Please refer to ISO 3166-1-alpha-2 for a list.	[A-Z]	2,2	o recommended – 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 recommended – when initiating 3D secure transaction
d1	Cardholder IP Address The IP address of the server that is connecting to the Shift4 gateway should always be sent in Card-Present transactions.	[0-9\.]	7,15	c, m for Visa 3ds transactions
d2	Echo parameter Any value up to 128 chars long transmitted with a request will be returned within the response to this parameter. Note: No plaintext cardholder data should be provided in this field.	[a-zA-Z0-9]	3,128	o
f21	Boolean field specifying whether the fraud protection service check should be bypassed. Value Description 0 Send for a fraud check. (default value) 1 Do not send for a fraud check Only available to merchants using the Smart Guard fraud protection service	[0-1]	1,1	o(n/a for [6])
f22	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.	[0-9]	0,4	o(n/a for [6])

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
h3	Sub-Merchant ID The Merchant ID of a sub-merchant belonging to a Payment Facilitator Refer to Shift4 Payment Gateway: Processors Specification to learn which Payment Processors support Payment Facilitators.	[0-9]	1,15	c (Payment Facilitators)
h8	Sub-Merchant's telephone number	[0-9\-\.]	5,32	o
h9	Merchant Reference Number 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.	[a-zA-Z0-9]	1,32	o

<table>
<tr><th>Name</th><th>Description</th><th>Type</th><th>Length (min,max)</th><th>Stand-Alone Operations [1] [2] [6]</th></tr>
<tr><td>h15</td><td>Seller Information
This field contains seller information. When using this field, “Seller ID” is mandatory. The ID should be a unique identifier such as the seller name or an internal registration number.
Populate these fields with the following information, delimited by “|”.
Note: This field is used by marketplaces. Additional marketplace requirements and reporting guidelines appear on the “ Marketplace Guideline” guide in Shift4’s developer’s portal.

Field — Type — Length (min, max)
Seller ID — [a-zA-Z0-9\-] — 4,64
Seller country — [A-Z] — 3,3
Seller city — [a-zA-Z\-] — 3,30
Seller street — [a-zA-Z0-9\-] — 4,50
Seller postal code — [a-zA-Z0-9\-] — 1,9
Seller state — [a-zA-Z0-9] — 3,3</td><td>[a-zA-Z0-9\-\|]</td><td>9,164</td><td>c ([1], only)</td></tr>
<tr><td>i1</td><td>Transaction Free Text description</td><td>Text</td><td>5,64</td><td>o</td></tr>
<tr><td>i2</td><td>Billing Descriptor
The descriptor that appears on the cardholder's statement
Please refer to Shift4 Payment Gateway: Processors Specification to learn which Payment Processors support the dynamic descriptor feature. The i2 parameter will be ignored if the processor does not support Dynamic Descriptors.</td><td>Text</td><td>1,39</td><td>o</td></tr>
</table>

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
i8	3D Secure Data Composed of 3 different parameters delimited by a colon: 1. ECI 2. CAVV/AAV 3. XID Refer to Appendix J: How to Provide 3D Secure Data on the i8 Parameter Refer to Shift4 Payment Gateway: Processors Specification to learn whether the 3D secure service is supported and which Payment Processors support the transfer of 3DS information. A transmitted i8 will not be routed to Payment Processors that do not support this feature. Furthermore, the transaction will be rejected by the Shift4 Gateway if no optional Processor is found. Use this field when the 3D secure process is performed prior to payment initiation (for example with a third-party 3D Secure provider)	[a-zA-Z0-9\:\=\+]	10,128	o
3ds_version	Indicates the 3D Secure protocol version Possible values: 1.0 2.0 2.1.0 2.2.0	[0-9]	3,5	c (m if using i8)
3ds_dstrxid	3DS Directory server transaction ID. Must be sent if 3ds_version = 2.0 or higher and i8 is used. Refer to Appendix J: How to Provide 3D Secure Data on the i8 Parameter	[0-9A-Za-z,-]	36	c (m if 3ds_version = 2.0 or higher)
j1	Primary Account Recipient's date of birth	YYYYMMDD		c (6012 UK merchant)

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
j2	Masked PAN or merchant system account number. Should contain either the first 6 or last 4 digits of the Primary Account Recipient's PAN or another account identifier used by the merchant. May contain asterisks.	[a-zA-Z0-9*]	8,8	c (6012 UK merchant)
j3	Primary Account Recipient's Postal Code	[a-zA-Z0-9 /-/]	2,6	c (6012 UK merchant)
j4	Primary Account Recipient's partial surname	[a-zA-Z*]	2,6	c (6012 UK merchant)
j5	Funds Recipient's First name	[a-zA-Z0-9\ \-]	1,30	c (m for AFT)
j6	Funds Recipient's Street Address	['"0-9A-Za-z]	1,30	c (m for AFT)
j7	Funds Recipient's City	[‘”0-9A-Za-z]	1,25	c (m for AFT)
j8	Funds Recipient's State/Province Code	[0-9A-Za-z]	2,3	c (m for AFT, in US or Canada)
j9	Funds Recipient's Country Code	[A-Z]	3,3	c (m for AFT)
j10	Funds Recipient's Phone Number	[0-9-]	1,20	o
j11	Funds Recipient's Date of Birth	MMDDYYYY	8,8	o
j12	Funds Recipient Postal Code	[a-zA-Z0-9 /-/]	1,10	o
j13	Funds Recipient Surname	[a-zA-Z0-9\ \-]	1,30	c (m for AFT)
r1	Indicates the selected Processor for the specific transaction. The transaction is routed according to the transmitted value. See Appendix G for the list of possible values.	[a-zA-Z0-9]	0,9	o(n/a for [6])
r2	Indicates the Processor target MID for the specific transaction. The transaction is routed according to the transmitted value.	[a-zA-Z0-9]	0,32	o(n/a for [6])
r3	The routing sequence number.	[1-9]	1,2	o

Name	Description	Type	Length (min,max)	Stand-Alone Operations [1] [2] [6]
3ds_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 • 04: Only initiate the 3DS Adviser service. Relevant only for op code 98. For additional information about the 3D Secure process, see Appendix I: 3D Secure. **Note**: If the transaction contains both the 3ds_initiate parameter and the i8 parameter, the transaction will be declined.	[0-3]	2,2	o (default value: 02)
token_eci	ECI value returned from the token decryption process	[0-9]	2,2	c (m if transaction is scheme token based and b21 is sent)
token_crypto	CAVV/AAV value returned from the token decryption process	[A-Za-z0-9]	40,40	c (m if transaction is scheme token based and b21 is sent)

Referral Operations

The Referral group includes six operations for transmitting basic Captures, Refunds and Voids.

List of Referral Operations	
[3]	Capture
[4]	Authorisation Void

List of Referral Operations	
[5]	Referral Credit
[7]	Sale Void
[8]	Refund Void
[9]	Capture Void
[20]	Incremental Authorisation

[3] - Capture

A Capture refers to a previous Authorisation transaction and should be sent after a successful Authorisation. It also includes the transaction in the next clearing file.

Note: A Capture should only be sent after a successful Authorisation

[4] - Authorisation Void

An authorisation void initiates an online full or partial Authorisation reversal.

Condition: Can be sent if a previous [2] operation has been sent and if no [3] operation has already been sent

[5] - Referral Credit

A Referral Credit initiates a refund of a previously Captured transaction.

[7] - Sale Void

A Sale Void initiates an online Authorisation reversal. As a Sale includes both an Authorisation and a Capture, this operation also cancels the Capture operation.

[8] - Refund Void

A Refund Void cancels a previous Refund transaction (i.e., removes it from the clearing file). A Refund Void can be used for revoking operations [5] and [15].

[9] - Capture Void

A Capture Void voids a previously Captured transaction (i.e., removes it from the clearing file).

Note:

A void of sale/refund/capture operations can only be transmitted within 24 hours of the original transaction

[20] – Incremental Authorisation

An incremental authorisation initiates an online authorisation request to increase the amount of a previous authorisation transaction.

Required Parameters

Name	Description	Type	Length	Referral Operations [3] [4] [5] [7] [8] [9] [20]
M	*Shift4* assigned gateway merchant ID	[A-Z0-9_]	3,6	m
K	Unique cipher used for authenticating requests Refer to Appendix A: Message Cipher for further details on generating the cipher.	[0-9A-Za-z]	1,32	m
O	Operation Code The operation code is used for determining the requested service. See List of Referral Operations.	[0-9]	1,3	m
a1	Request ID A unique transaction Reference Number, which should be unique to each transaction and to each MID. May be used when corresponding with the Payment Processor or when reconciling transactions. Note: No plaintext cardholder data should be provided in this field.	[A-Za-z0-9-]	1,32	m
a2	Payment Source Type Valid options are: 2 Online Order (default value) 3 Telephone Order 4 Mail Order 5 Virtual Terminal	[0-9]	1,2	o

Name	Description	Type	Length	Referral Operations [3] [4] [5] [7] [8] [9] [20]
a4	Requested billing amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no exponents should be formatted according to their currency requirements. Refer to Appendix H: Transaction Currencies for more information. The amount can be transmitted as part of a referral transaction in order to indicate a partial amount (in case of a partial void, a partial refund or a partial capture) or to indicate an additional amount (in case of incremental authorisation). In all other cases, a referral transaction defaults to the full amount transmitted in the original transaction's a4 parameter.	[0-9]	1,12	m
a5	Transaction Currency Indicates the currency that should be used in the transaction (every currency used must be preconfigured on the *Shift4* platform). Refer to ISO 4217-alpha-3 for further details	[A-Z]	3,3	m
a6	Transaction date (current local date of the transaction)	yyMMdd	6,6	o
a7	Transaction time (current local time of the transaction)	HHmmss	6,6	o

Name	Description	Type	Length	Referral Operations [3] [4] [5] [7] [8] [9] [20]
a9	Transaction type. Valid values are: Value Description 1 First standing order 2 Subsequent standing order 5 Card-Only Validation 6 Straight Operation 8 Unscheduled Card-on-File transactions initiated by the merchant. Use with [20] – Incremental authorisation 9 Unscheduled Card-on-File transactions initiated by the cardholder 10 Card validations for an unscheduled Card-on-File 11 First Subscription 12 Subscription By default, the transaction type is considered a straight operation unless specified otherwise.	[0-9]	1,2	o
b3	Card expiration month Two-digit number (*mm* format)	[0-9]	2,2	c for [5]
b4	Card expiration year Two-digit number (yy format)	[0-9]	2,2	c for [5]
d1	Cardholder IP Address The IP address of the server that is connecting to the *Shift4* gateway should always be sent for Card-Present transactions.	[0-9\.]	7,15	c, m for Visa 3ds transactions
d2	Echo parameter Any value up to 128 bytes long transmitted within a request will be returned within the response to this parameter. Note: No plaintext cardholder data should be provided in this field.	Text	3,128	o

Name	Description	Type	Length	Referral Operations [3] [4] [5] [7] [8] [9] [20]
g2	Response ID The z1 parameter from a corresponding past transaction.	[a-zA-Z0-9]	1,32	m
g3	Authorisation Code The z4 parameter from a corresponding past transaction.	[a-zA-Z0-9]	1,10	o
g4	Request ID The a1 parameter from a corresponding past transaction.	[0-9A-Za-z]	1,32	o
g6	Initial transaction ID The z50 parameter that was received in the original transaction response. Must be sent to ensure the transaction is considered an MIT transaction. Note: The card schemes require that each subsequent transaction includes a proper 'initial transaction id' on the g6 parameter. Generic values will no longer be accepted. This applies to transactions from all times. . If you do not have this value, work with your customers to get a new original transaction authorised and authenticated.	[0-9A-Za-z]	13,15	o (m if a9=2 or 8)
h9	Merchant reference number This optional field is a secondary transaction reference number which can be transmitted in addition to a1. Note: No plaintext cardholder data should be provided in this field.	Text	1,32	o

Name	Description	Type	Length	Referral Operations [3] [4] [5] [7] [8] [9] [20]
h15	Seller Information This field contains seller information. When using this field, “Seller ID” is mandatory. The ID should be a unique identifier such as the seller name or an internal registration number. Populate these fields with the following information, delimited by “|”. Note: This field is used by marketplaces. Field / Type / Length (min, max) Seller ID / [a-zA-Z0-9\-] / 4,64 Seller country / [A-Z] / 3,3 Seller city / [a-zA-Z\-] / 3,30 Seller street / [a-zA-Z0-9\-] / 4,50 Seller postal code / [a-zA-Z0-9\-] / 1,9 Seller state / [a-zA-Z0-9] / 3,3	[a-zA-Z0-9\-|]	9,164	c (mandatory for [3] only)
i2	Billing Descriptor The Descriptor that appears on the cardholder's statement. Refer to Shift4 Payment Gateway: Processors Specification to learn whether the Dynamic Descriptor feature is supported. The i2 parameter will be ignored if the processor does not support Dynamic Descriptors.	Text	1,39	o

Token (Card-on-file) Operations

This group of operations enables eCommerce ‘quick checkout’ and recurring transactions using the *Shift4* token engine.

Token (Card-on-file) Operations	
[10]	Create Token
[23]	Create Token with Sale
[28]	Create Token - Auth
[29]	Create Token – Capture
[11]	Use Token – Sale
[12]	Use Token – Auth
[13]	Use Token – Capture
[24]	Use Token – Recurring Sale
[32]	Use Token - Recurring Auth
[33]	Use Token – Recurring Capture
[14]	Token Auth Void
[15]	Token Referral Credit
[16]	Block Token

Create Token Operations

[10] Create Token

A Create Token operation initiates a card validation transaction and then, if successful, stores the card's details in the tokenisation engine.

Note:

- This transaction performs card validation using the inimal transaction amount allowed by the selected payment processr, regardless of the amount transmitted in the request.
- A successful request returns a value of '0' (zero) in the z2 paramter and '85' "No Reason to Decline (Valid for all Zero-Amount Transactions)" in the z6 parameter

[23] Create Token with Sale

Creates a token together with an initiation of a Sale [1] transaction

[28] Create Token – Auth

Creates a token together with an initiation of an Authorisation [2] transaction

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
M	*Shift4* assigned Gateway Merchant ID	[A-Z0-9_]	3,6	m
K	Unique cipher used for authenticating requests. Refer to Appendix A: Message Cipher for further details on generating the cipher.	[0-9A-Za-z]	1,32	m
O	Operation Code The operation code is used for determining the requested service. See the list in Create Token Operations.	[0-9]	1,3	m
a1	Request ID A unique transaction reference number that should be unique to each transaction and to each MID. May be used when corresponding with the payment processor or when reconciling transactions. Note: No plaintext cardholder data should be provided in this field.	[A-Za-z0-9-]	1,32	m

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
a2	Payment source Type Valid options are: 2 Online Order (default value) 3 Telephone Order 4 Mail Order 5 Virtual Terminal	[0-9]	1,2	o
a4	Requested Billing Amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no exponents should be formatted according to their currency requirements. Refer to Appendix H: Transaction Currencies for more details The minimum transaction value should be 0.01 EUR (or the equivalent or EUR 0.01 in another currency), otherwise the request is rejected.	[0-9]	1,12	m
a5	Transaction Currency Indicates the currency that should be used in the transaction (every currency used must be preconfigured on the *Shift4* platform). Refer to ISO 4217-alpha-3 for further information.	[A-Z]	3,3	m
a6	Transaction date (local date of the transaction)	yyMMdd	6,6	o
a7	Transaction time (local time of the transaction)	HHmmss	6,6	o
a8	Merchant Invoice ID Only required for subscription transactions.	text	1,16	c (required for [23], [28])
a9	Transaction Type. Valid values are: **Value** **Description** 1 First standing order 2 Subsequent standing order 5 Card-Only Validation 6 Straight Operation	[0-9]	1,2	o

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
	8 Unscheduled Card-on-File transactions initiated by the merchant 9 Unscheduled Card-on-File transactions initiated by the cardholder 10 Card validations for an unscheduled Card-on-File 11 First subscription 12 Subscription Note: • By default, the transaction type is considered a straight operation unless specified otherwise. • Transmitting a9 with a value of 5 for Operation Code 23 triggers a rejection response. • Transmitting a9 with a value of 2 for Operation Code 28 triggers a rejection response			
a10	Authorisation Type: **Value** **Description** 1 Final Authorisation (default value) 2 Pre-Authorisation 3 Deferred Authorisation Transactions referring to Pre-Authorisations must include an a4 parameter.	[1-2]	1,1	c (mandatory for [23], [28] only)
a11	Multiple Capture tag Indicates the number of expected Captures • Only supported in Card-not-Present transactions • Default value is 1 • Max value is 98 • Min value is 2	[0-9]	1,2	c (mandatory for [28] only)
a14	Partial Authorisation tag	[0,1]	1,1	c (mandatory for [28] only)

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
	This request parameter indicates to the issuer whether you are willing to accept partial authorisation approval. Possible values: 0 – Full authorisation only (default) 1 – Partial authorisation also accepted			
b1	PAN – Primary Account Number	[0-9]	8,19	m
b3	Card expiration month Two-digit number (*mm* format)	[0-9]	2,2	m
b4	Card expiration year Two-digit number (*yy* format)	[0-9]	2,2	m
b5	Card Security Code (CVV / CVC) as printed on the card	[0-9]	3,3	m
b21	Passthrough wallet indicator Indicates whether the transaction originally issued from a passthrough wallet supported by Shift4. Possible values: • applepay: for Apple Pay • googlepay: for Google Pay • vts_mdes_token: for VTS and M4M (MDES for Merchants) token-based transactions • samsungpay: for Samsung Pay	[A-Za-z\ ]	8-14	c (mandatory if transaction was originally an Apple Pay, Google Pay, Samsung Pay or VTS/M4M transaction)
c1	Cardholder's full name NOTE: the minimum length of this field is five characters. If the cardholder provides a name that is less than five characters long, you must either add additional non-space characters to the name (e.g. Mr. Lu) or not transmit the field	[\ a-zA-Z]	5,45	c recommended – when initiating 3D secure transaction, m for Visa 3ds transactions
c2	Cardholder's contact phone number Note: For Visa 3ds transactions cardholder's phone number or email are mandatory.	[0-9\-\.]	5,32	c m for Visa 3ds transactions, o if c3 is sent. For 3DS transactions always

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
				include 3ds_homephonecountry..
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	m
c4	Cardholder Billing Address street number If the processor supports AVS then the transmission of this parameter will trigger the AVS system. Note that the street number should be omitted from the c5 parameter if this parameter is transmitted.	[0-9]	1,16	o recommended – when initiating 3D secure transaction
c5	Cardholder Billing Address street name The street number should not be included here if the c4 parameter is transmitted.	[a-zA-Z0-9\ \-]	4,50	o recommended – when initiating 3D secure transaction
c7	Cardholder Billing Address city name	[a-zA-Z\ \-]	3,30	o recommended – when initiating 3D secure transaction
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]	3,30	o recommended – when initiating 3D secure transaction
c9	Cardholder Billing Address Country Code Refer to ISO 3166-1-alpha-2 for a reference list.	[A-Z]	2,2	o recommended – when initiating 3D secure transaction
c10	Cardholder Billing Address Postal/ZIP Code If transmitted, this value is sent to the issuer and will be part of the issuer's AVS checks Note: not all Payment Processors support AVS checks). Please refer to *Shift4 Payment Gateway: Processors Specification* for further details.	[a-zA-Z0-9\ \-]	1,9	c (required for [23], [28]) recommended – when initiating 3D secure transaction

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
d1	Cardholder IP Address The IP address of the server that is connecting to the *Shift4* gateway should always be transmitted in Card-Present transactions.	[0-9\.]	7,15	m
d2	Echo parameter Any value up to 128 bytes long transmitted within a request will be returned within the response to this parameter. Note: No plaintext cardholder data should be provided in this field.	Text	3,128	o
f21	Boolean field specifying whether the fraud protection service check should be bypassed. **Value** **Description** 0 Send for a fraud check. (default value) 1 Do not send for a fraud check Only available to merchants using the Smart Guard fraud protection service	[0-1]	1,1	o
f22	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.	[0-9]	0,4	o
h3	Sub-Merchant ID The merchant ID of a sub-merchant belonging to a Payment Facilitator Refer to *Shift4 Payment Gateway: Processors Specification* to learn which Payment Facilitators are supported.	[0-9]	1,15	c (Payment Facilitators)
h9	Merchant Reference Number This optional field is a secondary transaction reference number which can be sent alongside a1. Note: No plaintext cardholder data should be provided in this field.	Text	1,32	o

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
h15	Seller Information This field contains seller information. When using this field, “Seller ID” is mandatory. The ID should be a unique identifier such as the seller name or an internal registration number. Populate these fields with the following information, delimited by “|”. Note: This field is used by marketplaces. **Field / Type / Length (min, max)** Seller ID / [a-zA-Z0-9\-] / 4,64 Seller country / [A-Z] / 3,3 Seller city / [a-zA-Z\-] / 3,30 Seller street / [a-zA-Z0-9\-] / 4,50 Seller postal code / [a-zA-Z0-9\-] / 1,9 Seller state / [a-zA-Z0-9] / 3,3	[a-zA-Z0-9\-|]	9,164	c ([23]only)
i1	Transaction Free Text Description	Text	5,64	o
i2	Billing Descriptor The Descriptor that appears on the cardholder's statement. Refer to *Shift4 Payment Gateway: Processors Specification* to learn whether the Dynamic Descriptor feature is supported. The i2 parameter will be ignored if the processor does not support Dynamic Descriptors.	Text	1,39	o
i8	3D Secure Data Compose of 3 different parameters delimited by a colon: ECI CAVV/AAV XID	[a-zA-Z0-9\:\=\+]	10,128	o

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
	Refer to Appendix J: How to provide 3D Secure Data on the i8 Parameter for more details Refer to *Shift4 Payment Gateway: Processors Specification* to learn which Payment Processors support the transfer of 3DS information. A transmitted i8 will not be routed to Payment Processors that do not support this feature. Furthermore, the transaction will be rejected by the *Shift4* gateway if no optional Processor is found.			
3ds_version	Indicates the 3D Secure protocol version Possible values: • 1.0 • 2.0 • 2.1.0 • 2.2.0	[0-9]	3,5	c (m if using i8)
3ds_dstrxid	3DS Directory server transaction ID. Must be sent if 3ds_version = 2.0 or higher and i8 is used. Refer to Appendix J: How to Provide 3D Secure Data on the i8 Parameter	[0-9A-Za-z,-]	36	c (m if 3ds_version = 2.0 or higher)
j1	Primary Account Recipient's date of birth	YYYYMMDD		c (6012 in UK)
j2	Masked PAN or account number from merchant systems. Should contain either the first 6 or last 4 digits of the primary account recipient's PAN or another account identifier utilised by the merchant. May contain asterisks.	[a-zA-Z0-9*]	8,8	c (6012 in UK)
j3	Primary Account Recipient's Postal Code	[a-zA-Z0-9 /-/]	2,6	c (6012 in UK)
j4	Primary Account Recipient's partial surname	[a-zA-Z*]	2,6	c (6012 in UK)
j5	Funds Recipient's First Name	[-''A-Za-z]	1,30	o

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
j6	Funds Recipient's Street Address	['"0-9A-Za-z]	1,30	o
j7	Funds Recipient's City	['"0-9A-Za-z]	1,25	o
j8	Funds Recipient's State/Province Code	[0-9A-Za-z]	2,3	o
j9	Funds Recipient's Country Code	[A-Z]	3,3	o
j10	Funds Recipient's Phone Number	[0-9-]	1,20	o
j11	Funds Recipient's Date of Birth	MMDDYYYY	8,8	o
j12	Funds Recipient's Postal Code	[a-zA-Z0-9-]	1,10	o
j13	Funds Recipient's Surname	[A-Za-z]	1,30	o
r1	Chooses the Processor for the specific transaction. The transaction will then be routed according to the transmitted value. See Appendix G for the list of possible values.	[a-zA-Z0-9]	0,9	o
r2	Chooses the Processor MID for the specific transaction. The transaction will then be routed according to the transmitted value.	[a-zA-Z0-9]	0,32	o
r3	Routing sequence number	[1-9]	12	o
3ds_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 3D Secure 03: Initiate 3D Secure according to the 3DS Adviser result 04: Only initiate the 3DS Adviser service. Relevant only for op code 98. For additional information about the 3D secure process, see Appendix I: 3D Secure.	[0-3]	2,2	o (default value: 02)

Name	Description	Type	Length	Create Token Operations [10] [23] [28]
	Note: If the transaction contains both the 3ds_initiate parameter and the i8 parameter, the transaction will be declined.			
token_eci	ECI value returned from the token decryption process	[0-9]	2,2	c (m if transaction is scheme token based and b21 is sent)
token_crypto	CAVV/AAV value returned from the token decryption process	[A-Za-z0-9]	40,40	c (m if transaction is scheme token based and b21 is sent)

Use Token Operations

[11] Use Token – Sale

This operation uses stored card details to generate a Sale [1] transaction

[12] Use Token – Auth

This operation uses stored card details to generate an Authorisation [2] transaction

[24] Use Token – Recurring Sale

This operation uses a previously created token to generate a Recurring Sale [1] transaction

[32] Use Token - Recurring Auth

This operation uses a previously created token to generate a Recurring Authorisation [2] transaction

[16] Block Token

This operation makes a token unusable, so it cannot be used for Sales, Authorisations, Credits, etc. Blocked tokens are still allowed to process Refunds and Captures of any transactions authorised or processed prior to the Block Token operation.

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
M	Shift4 assigned gateway Merchant ID	[A-Z0-9_]	3,6	m

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
K	Unique cipher used for authenticating requests Refer to Appendix A: Message Cipher for further details on generating the cipher.	[0-9A-Za-z]	1,32	m
O	Operation Code The operation code is used for determining the requested service. See the list in Use Token Operations	[0-9]	1,3	m
a1	Request ID A unique Transaction Reference Number, which should be unique to each transaction and to each MID. May be used when corresponding with the Payment Processor or when reconciling transactions. Note: No plaintext cardholder data should be provided in this field.	[\-0-9A-Za-z]	1,32	m
a2	Payment Source Type Valid options are: 2 Online Order (default value) 3 Telephone Order 4 Mail Order 5 Virtual Terminal	[0-9]	1,2	o
a4	Requested Billing Amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no exponents should be formatted according to their currency requirements. The minimum transaction value should be 0.01 EUR (or the equivalent or EUR 0.01 in another currency), otherwise the request is rejected. Refer to Appendix H: Transaction Currencies for more details.	[0-9]	1,12	m (required for [11], [12], [24], [32]) Not required for [16]
a5	Transaction Currency	[A-Z]	3,3	m

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
	Indicates the currency that should be used in the transaction (every currency used must be preconfigured on the Shift4 platform). Refer to ISO 4217-alpha-3 for further information.			
a6	Transaction date (local date of the transaction)	yyMMdd	6,6	o
a7	Transaction time (local time of the transaction)	HHmmss	6,6	o
a8	Merchant Invoice ID Only required for subscription transactions.	text	1,16	o
a9	Transaction Type. Valid values are: Value — Description 1 — First standing order 2 — Subsequent standing order 5 — Card-Only Validation 6 — Straight Operation 8 — Unscheduled Card-on-File transactions initiated by the merchant 9 — Unscheduled Card-on-File transactions initiated by the cardholder 10 — Card validations for an unscheduled Card-on-File 11 — First Subscription 12 — Subscription Note: By default, the transaction type is considered a straight operation unless specified otherwise.	[0-9]	1,2	c (mandatory for [24], [32] only)

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
a10	Authorisation Type: 1. Final Authorisation (default value) 2. Pre- Authorisation 3. Deferred Authorisation Transactions referring to Pre-Authorisations must include the a4 parameter.	[1-3]	1,1	o ([11],[12],[24] ,[32] only)
a11	Multiple Capture tag Indicates the number of expected Captures Only supported in Card-not-Present transactions Default value is 1 Max value is 98 Min value is 2	[0-9]	1,2	o ([12],[32] only)
a14	Partial Authorisation tag This request parameter indicates to the issuer whether you are willing to accept partial authorisation approval. Possible values: 0 – Full authorisation only (default) 1 – Partial authorisation also accepted	[0,1]	1,1	o ([12], [32] only)
d1	Cardholder's IP Address The IP address of the server that is connecting to the Shift4 Gateway should always be sent for Card-Present transactions.	[0-9\.]	7,15	c, m for Visa 3ds transactions
d2	Echo parameter Any value up to 128 bytes long transmitted within a request will be returned within the response to this parameter.	Text	3,128	o

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
	Note: No plaintext cardholder data should be provided in this field.			
g1	Token Shift4-generated Token that refers to a stored card profile.	[a-zA-Z0-9]	1,32	m
g6	Initial transaction ID The z50 parameter that was received in the original transaction response. Must be sent to ensure the transaction is considered an MIT transaction. Note: The schemes require that each subsequent transaction includes a proper 'initial transaction id' on the g6 parameter. Generic values will no longer be accepted. This applies to transactions from all times. If you do not have this value, work with your customers to get a new original transaction authorised and authenticated.	[0-9A-Za-z]	13,15	o (m if a9=2 or 8)
h9	Merchant Reference Number This optional field is a secondary transaction reference number which can be transmitted alongside an a1 parameter. Note: No plaintext cardholder data should be provided in this field.	Text	1,32	o
h15	Seller Information This field contains seller information. When using this field, "Seller ID" is mandatory. The ID should be a unique identifier such as the seller name or an internal registration number. Populate these fields with the following information, delimited by "|". Note: This field is used by marketplaces.	[a-zA-Z0-9\-\\|]	9,164	c ([11], , [24], only)

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
	Field / **Type** / **Length (min, max)** Seller ID / [a-zA-Z0-9\-] / 4,64 Seller country / [A-Z] / 3,3 Seller city / [a-zA-Z\-] / 3,30 Seller street / [a-zA-Z0-9\-] / 4,50 Seller postal code / [a-zA-Z0-9\-] / 1,9 Seller state / [a-zA-Z0-9] / 3,3			
i2	Billing Descriptor The Descriptor that appears on the cardholder's statement. Refer to your *Processor Specifications* document to learn whether the Dynamic Descriptor feature is supported. The i2 parameter will be ignored if the Processor does not support Dynamic Descriptors	Text	1,39	o (Not required for [16])
j5	Funds Recipient's First name	[-''A-Za-z]	1,30	o
j6	Funds Recipient's Street Address	['"0-9A-Za-z]	1,30	o
j7	Funds Recipient's City	['"0-9A-Za-z]	1,25	o
j8	Funds Recipient's State/Province Code	[0-9A-Za-z]	2,3	o
j9	Funds Recipient's Country Code	[A-Z]	3,3	o
j10	Funds Recipient's Phone Number	[0-9-]	1,20	o
j11	Funds Recipient's Date of Birth	MMDDYYYY	8,8	o
j12	Funds Recipient's Postal Code	[a-zA-Z0-9-]	1,10	o
j13	Funds Recipient's Surname	[A-Za-z]	1,30	o

Name	Description	Type	Length	Use Token Operations [11] [12] [16] [24] [32]
3ds_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 3D Secure 03: Initiate 3D Secure according to the 3DS Adviser result 04: Only initiate the 3DS Adviser service. Relevant only for op code 98. For additional information about the 3D Secure process, see Appendix I: 3D Secure Note: If the transaction contains both the 3ds_initiate parameter and the i8 parameter, the transaction will be declined.	[0-3]	2,2	o (default value: 02)

Referral Token Operations

[13] Use Token – Capture

This operation generates a Capture [3] that pertains to a previous operation [12] transaction.

Note:

This transaction type can only be transmitted if a previous [12] operation has already been transmitted

[14] Token Auth Void

This operation initiates the online Authorisation reversal of a previous [12] operation

Note:

This transaction type can only be transmitted if a previous [12] operation has already been transmitted

[15] Token Referral Credit

This operation generates a refund that pertains to a previous [13] or [11] operation

Note:

This transaction type can only be transmitted if a previous [11] or [13] operation has already been transmitted.

[29] Create Token – Capture

A Capture operation that pertains to a previous [28] operation transaction. This does not trigger the creation of another token.

Note:

This transaction type can only be transmitted if a previous [28] operation has already been transmitted.

[33] - Use Token – Recurring Capture

A Capture operation that pertains to a previous [32] operation transaction

Note:

This transaction type can only be transmitted if a previous [32] operation has already been transmitted

Name	Description	Type	Length	Referral Operations [13] [14] [15] [29] [33]
M	*Shift4* assigned Gateway Merchant ID	[A-Z0-9_]	3,6	m
K	Unique cipher for authenticating requests Refer to Appendix A: Message Cipher for further details on generating the cipher.	[0-9A-Za-z]	1,32	m
O	Operation Code The operation code is used for determining the requested service. See the list in Referral Token Operations.	[0-9]	1,3	m
a1	Request ID A unique Transaction Reference Number that should be unique to each transaction and to each MID. May be used when corresponding with the Payment Processor or when reconciling transactions. Note: No plaintext cardholder data should be provided in this field.	[\-0-9A-Za-z]	1,32	m
a2	Payment Source Type Valid options are: 2 Online Order (default value) 3 Telephone Order 4 Mail Order 5 Virtual Terminal	[0-9]	1,2	o
a4	Requested Billing Amount The amount value should not include a decimal point. Amounts in currencies that have two, three or no exponents should be formatted according to their currency requirements. The minimum transaction value should be 0.01 EUR (or the equivalent or EUR 0.01 in another currency), otherwise the request is rejected. Refer to Appendix H: Transaction Currencies for more details	[0-9]	1,12	o
a5	Presentment Currency	[A-Z]	3,3	o

Name	Description	Type	Length	Referral Operations [13] [14] [15] [29] [33]
	Indicates the presentment currency that should be used in the transaction (every currency used must be preconfigured on the *Shift4* platform). Refer to ISO 4217-alpha-3 for more details.			
a6	Transaction date (local date of the transaction)	yyMMdd	6,6	o
a7	Transaction time (local time of the transaction)	HHmmss	6,6	o
a9	Transaction Type. Valid values are: **Value** **Description** 1 First standing order 2 Subsequent standing order 5 Card-Only Validation 6 Straight Operation 8 Unscheduled Card-on-File transactions initiated by the merchant 9 Unscheduled Card-on-File transactions initiated by the cardholder 10 Card validations for an unscheduled Card-on-File 11 First subscription 12 Subscription Note: • By default, the transaction type is considered a straight operation unless specified otherwise. • Sending a9 with the value 5 for operation codes 29/33 will trigger a rejection response. The Gateway will also reject the a9 parameter if it does not match the original operation code's a9 value.	[0-9]	1,2	o ([14], [29], [33] only)
b3	Card expiration month	[0-9]	2,2	o for [15]

Name	Description	Type	Length	Referral Operations [13] [14] [15] [29] [33]
	Two-digit number (*mm* format)			n/a for else
b4	Card expiration year Two-digit number (*yy* format)	[0-9]	2,2	o for [15] n/a for else
d1	Cardholder IP Address The IP Address of the server that is connecting to the *Shift4* gateway should always be sent in Card-Present transactions.	[0-9\.]	7,15	c, m for Visa 3ds transactions
d2	Echo parameter Any value up to 128 bytes long transmitted within a request will be returned within the response to this parameter. Note: No plaintext cardholder data should be provided in this field.	Text	3,128	o
g1	Token A *Shift4*-generated Token that references a stored card profile.	[a-zA-Z0-9]	1,32	o
g2	Response ID The z1 parameter from a corresponding past transaction.	[a-zA-Z0-9]	1,32	m
g3	Authorisation Code The z4 parameter from a corresponding past transaction.	[a-zA-Z0-9]	1,10	o
g4	Request ID The a1 parameter from a corresponding past transaction.	[0-9A-Za-z]	1,32	o
g6	Initial transaction ID The z50 parameter that was received in the original transaction response. Must be sent to ensure the transaction is considered an MIT transaction. **Note**: The schemes require that each subsequent transaction includes a proper 'initial transaction id' on the g6 parameter. Generic values will no longer be accepted. This applies	[0-9A-Za-z]	13,15	o (m if a9=2 or 8)

Name	Description	Type	Length	Referral Operations [13] [14] [15] [29] [33]
	to transactions from all times. . If you do not have this value, work with your customers to get a new original transaction authorised and authenticated.			
h9	Merchant Reference Number This optional field is a secondary transaction reference number which can be sent alongside a1. Note: No plaintext cardholder data should be provided in this field.	Text	1,32	o
h15	Seller Information This field contains seller information. When using this field, "Seller ID" is mandatory. The ID should be a unique identifier such as the seller name or an internal registration number. Populate these fields with the following information, delimited by "|". **Note:** This field is used by marketplaces. **Field** / **Type** / **Length (min, max)** Seller ID / [a-zA-Z0-9\-] / 4,64 Seller country / [A-Z] / 3,3 Seller city / [a-zA-Z\-] / 3,30 Seller street / [a-zA-Z0-9\-] / 4,50 Seller postal code / [a-zA-Z0-9\-] / 1,9 Seller state / [a-zA-Z0-9] / 3,3	[a-zA-Z0-9\-|]	9,164	c ([13], [29], [33] only)
i1	Transaction Free Text Description	Text	5,64	o

Special Operations

This group of operations includes special transaction types that are only required for specific business types or industries or in specific business scenarios.

Special Operations	
[34]	Referral CFT (Credit Fund Transfer)
[35]	Independent CFT (Credit Fund Transfer)
[37]	Create Independent CFT Token
[38]	Use Independent CFT Token
[98]	Authenticate Cardholder without payment (3D Secure)
[88]	Create Token and Authenticate Cardholder without payment (3D Secure)
[89]	Use Token and Authenticate Cardholder without payment (3D Secure)

[34] - Referral CFT (Credit Fund Transfer)

Referral CFT is used to credit funds to a cardholder, where the funds being credited refer to a previous original Sale or Capture transaction. The use of this operation code requires prior approval from Shift4; contact your account manager for more details.

This type of CFT is commonly used in gaming businesses (MCC 7994), gambling businesses (MCC 7995) and other industries such as Forex businesses (MCC 6211).

Note:

The original transaction that is referred to must be successfully authorized and captured in order to process a [34] – Referal CFT. Otherwise the referral CFT transaction will be declined.

[35] - Independent CFT (Credit Fund Transfer)

Independent CFT is used to credit funds to a cardholder when the funds being credited do **not** refer to a previous original Sale of Capture transaction. The use of this operation code requires prior approval from Shift4; contact your account manager for more details.

[37] – Create Independent CFT Token

Creates a token as part of the process of initiating an independent CFT transaction [35].

[38] – Use Independent CFT Token

Uses stored card details to initiate an Independent CFT token [35] transaction.

Note:

According to the card scheme's rules, the payout transactions are final and cannot be voided (except for Mastercard transaction processed with MCC 7995).

This means you should not send operation [8] – Refund Void for payout transactions initiated and of the following operation codes:

[34] – Referral CFT

[35] – Independent CFT

[37] – Create token – Independent CFT

[38] – Use token – Independent CFT

Attempting to void these transaction will result in a decline

[98] - Authenticate the cardholder with 3D secure without processing the payment

Use this operation code in cases you want to send a transaction to the Shift4 3D secure service without initiating a payment.

[88] Create Token and Authenticate Cardholder without payment (3D Secure)

Use this operation code in cases you want to create a token and send a transaction to the Shift4 3D Secure service without initiating a payment.

[89] Use Token and Authenticate Cardholder without payment (3D Secure)

Use this operation code in cases you want to use a token and send a transaction to the Shift4 3D Secure service without initiating a payment.

Name	Description	Referral CFT [34]	Independent CFT [35], [37]	Use Token Independent CFT [38]	3D Only [98]	Create Token 3D Only [88]	Use Token 3D Only [89]
M	Merchant ID	m	m	m	m	m	m
K	Package Signature	m	m	m	m	m	m
O	Operation Code	m	m	m	m	m	m
a1	Request ID	m	m	m	m	m	m
a2	Source Type ID	o	o	o	o	-	-
a4	Billing Amount	m	m	m	m	m	m

Name	Description	Referral CFT [34]	Independent CFT [35], [37]	Use Token Independent CFT [38]	3D Only [98]	Create Token 3D Only [88]	Use Token 3D Only [89]
a5	Billing Currency Code	m	m	m	m	m	m
a6	Transaction Date	o	o	o	o	o	o
a7	Transaction Time	o	o	o	o	o	o
a8	Merchant Order ID/Invoice	o	o	o	o	o	o
b1	Card Number	-	m	-	m	m	-
b3	Card Expiration Month (*mm*)	-	m	-	m	m	-
b4	Card Expiration Year (*yy*)	-	m	-	m	m	-
c1	Billing Contact Name	-	-	-	m	c	c
c2	Billing Contact Phone Number	-	-	-	c	c	c
c3	Billing Email Address	m	-	-	m	c	c
c4	Billing Street Number	-	-	-	o	o	o
c5	Billing Street Name	-	-	-	o	o	o
c7	Billing City Name	-	-	-	o	o	o
c8	Billing Territory ISO Code	-	-	-	o	o	o
c9	Billing Country ISO Code	-	-	-	o	o	o
c10	Billing Postal Code	-	-	-	o	o	o
d1	End User IP Address	o	m	m	m	c	co
d2	Echo	o	o	o	o	o	o

Name	Description	Referral CFT [34]	Independent CFT [35], [37]	Use Token Independent CFT [38]	3D Only [98]	Create Token 3D Only [88]	Use Token 3D Only [89]
g1	Shift4 assigned Token id	-	-	m	o	-	m
g2	Previous Response ID	m	-	-	-	-	-
g3	Previous Authorisation Code	o	-	-	-	-	-
g4	Previous Request ID	o	-	-	-	-	-
g6	Initial transaction ID	o	-	-	-	-	-
h9	Merchant Reference Number	o	o	o	o	o	o
i1	Transaction Free Text Description	o	o	-	o	o	o
i2	Statement Charge Descriptor	-	-	-	o	o	o
j5	Funds Recipient's First Name	c (m if was not sent on the original transaction)	m	m	-	-	-
j6	Funds Recipient's Street Address	m (when j9=CAN)	m (when j9=CAN)	m (when j9=CAN)	-	-	-
j7	Funds Recipient's City	m (when j9=CAN)	m (when j9=CAN)	m (when j9=CAN)	-	-	-
j8	Funds Recipient's State/Province Code	m (when j9=CAN)	m (when j9=CAN)	m (when j9=CAN)	-	-	-
j9	Funds Recipient's Country Code	m (when j9=CAN)	m (when j9=CAN)	m (when j9=CAN)	-	-	-
j10	Funds Recipient's Phone Number	o	o	o	-	-	-

Name	Description	Referral CFT [34]	Independent CFT [35], [37]	Use Token Independent CFT [38]	3D Only [98]	Create Token 3D Only [88]	Use Token 3D Only [89]
j11	Funds Recipient's Date of Birth	o	o	o	-	-	-
j12	Funds Recipient's Postal Code	o	o	o	-	-	-
j13	Funds Recipient's Surname	c (m if was not sent on the original transaction)	m	m	-	-	-
3ds_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 3D Secure 03: Initiate 3D Secure according to the 3DS Adviser result 04: Only initiate the 3DS Adviser service. Relevant only for op code 98. For additional information about the 3D Secure process,	-	o	o	o	m	m

Name	Description	Referral CFT [34]	Independent CFT [35], [37]	Use Token Independent CFT [38]	3D Only [98]	Create Token 3D Only [88]	Use Token 3D Only [89]
	see Appendix I: 3D Secure Note: If the transaction contains both the 3ds_initiate parameter and the i8 parameter, the transaction will be declined.						

Data Retrieval Operations

This group of operations includes data retrieval transaction types that are only required for specific business types or industries or in specific business scenarios.

[101] - Past Transaction Retrieval

Passes back the data pertaining to a previous transaction as currently available in the Shift4 payment gateway system.

NOTE: When the returned response to a [101] transaction is z2=11 the response should be interpreted as "the transaction in question is currently being processed. Please try again later".

[103] - Get Fraud Scoring

This operation allows you to send a transaction to the SmartGuard service in order to obtain a risk score. This operation is only available to merchants registered to *Shift4's* SmartGuard service.

[104] – Get Fast Funds Indicator

This operation enables you to send an independent query request for a specific card number (b1) in order to obtain information whether this card's issuer supports fast funds transfer. The response is provided in the z51 parameter.

[105] – Use Token Get Fast Funds Indicator

Enables you to send a query request for a specific Shift4 token (g1) in order to obtain information whether the referenced card's issuer supports fast funds transfer. The response is provided in the z51 parameter.

Name	Description	Retrieval Operation [101]	Get Fraud Scoring [103]	Get Fast Funds Indicator [104]	Use Token Get Fast Funds Indicator [105]
M	Merchant ID	m	m	m	m
K	Package Signature	m	m	m	m
O	Operation Code	m	m	m	m
a1	Request ID	m	m	m	m
a2	Source Type ID	-	o	-	-
a4	Billing Amount	-	m	-	-
a5	Billing Currency Code	o	m	-	-
a6	Transaction Date	-	o	-	-
a7	Transaction Time	-	o	-	-
a8	Merchant Order ID/Invoice	-	-	-	-
b1	Card Number	-	m	m	-
b3	Card Expiration Month (mm)	-	m	-	-
b4	Card Expiration Year (yy)	-	o	-	-
c1	Billing Contact Name	-	m	-	-
c2	Billing Contact Phone Number	-	m	-	-
c3	Billing Email Address	-	m	-	-
c4	Billing Street Number	-	c	-	-

Name	Description	Retrieval Operation [101]	Get Fraud Scoring [103]	Get Fast Funds Indicator [104]	Use Token Get Fast Funds Indicator [105]
c5	Billing Street Name	-	o	-	-
c7	Billing City Name	-	o	-	-
c8	Billing Territory ISO Code	-	o	-	-
c9	Billing Country ISO Code	-	o	-	-
c10	Billing Postal Code	-	o	-	-
d1	End User IP Address	-	o	-	-
d2	Echo	o	o	-	-
g1	Shift4 assigned Token id	-	-	-	m
g2	Previous Response ID	-	c	-	-
g3	Previous Authorisation Code	-	m	-	-
g4	Previous Request ID	m	o	-	-
g6	Initial transaction ID	-	-	-	-
h3	Sub merchant id	-	-	o	o
h9	Merchant Reference Number	o	-	-	-
i1	Transaction Free Text Description	-	-	-	-

Name	Description	Retrieval Operation [101]	Get Fraud Scoring [103]	Get Fast Funds Indicator [104]	Use Token Get Fast Funds Indicator [105]
i2	Statement Charge Descriptor	-	-	-	-
j5	Funds Recipient's First Name	-	-	-	-
j6	Funds Recipient's Street Address	-	-	-	-
j7	Funds Recipient's City	-	-	-	-
j8	Funds Recipient's State/Province Code	-	-	-	-
j9	Funds Recipient's Country Code	-	-	-	-
j10	Funds Recipient's Phone Number	-	-	-	-
j11	Funds Recipient's Date of Birth	-	-	-	-
j12	Funds Recipient's Postal Code	-	-	-	-
j13	Funds Recipient's Surname	-	-	-	-
3ds_initiate	Indicates whether to initiate the Shift4 3D Secure Authentication process. Possible values are:	-	-	-	-

Name	Description	Retrieval Operation [101]	Get Fraud Scoring [103]	Get Fast Funds Indicator [104]	Use Token Get Fast Funds Indicator [105]
	01: Initiate 3D Secure before completing the payment 02: Process payment without 3D Secure 03: Initiate 3D Secure according to the 3DS Adviser result 04: Only initiate the 3DS Adviser service. Relevant only for op code 98. For additional information about the 3D Secure process, see Appendix I: 3D Secure Note: If the transaction contains both the 3ds_initiate parameter and the i8 parameter, the transaction will be declined.				

Response Fields

The following API parameters are returned in the transaction response.

Note:

- Echo parameters are only returned in the transaction response if the respective parameters were sent in the request
- New response paramteres may be added in the future without prior notice. Make sure your implementation can support that

Name	Description	Type	Length
M	Shift4-assigned Gateway Merchant ID	[A-Z0-9_]	3,6
T	Transaction processing timestamp formatted as MM/dd/yyyy HH:mm:ss	timestamp	1,32
a1	Request ID as sent in the request	[\-0-9A-Za-z]	1,32
a2	Payment Source Type as sent in the request	[0-9]	1,2
a4	Requested Billing Amount as sent in the request	[0-9]	1,12
a6	Transaction date (local date of the transaction) as sent in the request	yyMMdd	6,6
a7	Transaction time (local time of the transaction) as sent in the request	HHmmss	6,6
a9	Transaction Type as sent in the request	[0,9]	1,2
b1	PAN – Primary Account Number. Masked as: ######****####	[0-9]	8,19
b2	Card type. Valid options are: Code Card Scheme 0 Unknown	[0-9]	1,2

Name	Description	Type	Length
	1 Visa 2 Mastercard 3 American Express 4 Isracard 9 Maestro 10 JCB 12 Discover 13 Diners 14 Cartes Bancaires		
b3	Card expiration month as sent in the request	[0-9]	2,2
b4	Card expiration year as sent in the request	[0-9]	2,2
b20	Payment Account Reference (PAR)	[a-zA-Z0-9]	29,29
c1	Cardholder's full name as sent in the request	[\ a-zA-Z]	5,45
d2	Echo parameter as sent in the request	Text	3,128
g1	Token *Shift4*-generated Token that refers to a stored card profile.	[a-zA-Z0-9]	1,32
g2	Response ID as sent in the request	[a-zA-Z0-9]	1,32
h3	Sub-Merchant ID as sent in the request	0-9	1,15
h9	Merchant Reference Number as sent in the request	Text	1,32
i1	Transaction Free Text Description as sent in the request	Text	5,64

Name	Description	Type	Length
j1	Primary Account Recipient's date of birth as sent in the request	YYYYMMDD	8,8
j2	Masked PAN or account number from merchant systems as sent in the request.	[a-zA-Z0-9*]	8,8
j3	Primary Account Recipient's Postal Code as sent in the request	[a-zA-Z0-9 /-/]	2,6
j4	Primary Account Recipient's partial surname as sent in the request	[a-zA-Z*]	2,6
z1	Shift4 Gateway Transaction ID The Transaction ID that uniquely identifies this transaction in the Shift4 gateway.	[a-zA-Z0-9]	1,32
z2	Gateway Response Code. A value of 05 means that the transactions were rejected by the processor. Refer to z6 to see the original response code Refer to Appendix B: Operation Result Codes for more information	[0-9-]	1,3
z3	Description of the operation's result	text	5,256
z4	Authorisation Code	[a-zA-Z0-9]	1,10
z5	Risk Score The fraud protection service's response. The transaction will be	[ABC0-9]	1,6

Name	Description	Type	Length
	rejected if the value of z5 is greater than or equal to the threshold defined in the merchant setup but will continue its flow if the value of z5 is lower than the merchant defined threshold. Refer to SmartGuard for more information.		
z6	Processing Response Reason Code. The original Processor response is provided in parameter z41. For more information, refer to Appendix D: Processing Response Reason Codes.	[A-Z0-9]	1,3
z9	AVS response The Address Verification Service (AVS) Authorisation response provided by the acquirer at the time of Authorisation. For more information, refer to Appendix C: AVS Response Codes.	[A-Z0-9]	1,2
z13	RRN The transaction Retrieval Reference Number (RRN) may be provided by the processor as an additional identifier of the transaction.	[a-zA-Z0-9]	1,32
z14	CVV2 response code Valid values are:	[A-Z]	1,1

Name	Description	Type	Length
	'M' - CVV2/CVC2 Matches 'N' – CVV2/CVC2 does not Match 'P' – Not processed 'S' – The CVV2 should be on the card but the merchant indicates it is not. 'U' – CVV2/CVC2 Unavailable – issuer does not support this parameter 'Y' – CVC1 Incorrect '1' - CVV2/CVC2 Unavailable – processor / card type does not support this parameter '2' - An unrecognised result code was returned by the processor '3' - No result code was returned by the processor.		
z15	Approved Billing Amount If the issuer approved a partial amount, the approved amount is indicated in this response parameter. The amount is provided in the same exponent and currency as the requested amount.	[0-9]	1,10
z16	Balance Response. For Card-Present transactions carried out with debit or prepaid	[0-9]	1,10

Name	Description	Type	Length
	cards, the issuer may choose to return the current balance of the associated account. The value of this balance will be returned in this field if provided by the issuer.		
z17	Balance Response Currency. If a balance response is provided (see notes relating to field z16 above), its currency will be returned in this parameter.	[A-Z0-9]	3,3
z21	Indicates the result of the transaction's transmission to the fraud-protection service. See Appendix E: z21 Possible Values for the list of all possible z21 result codes.	[0-9-]	1,3
z25	Indicates the updated amount of the transaction. Populated only in cases of changed amount such as authorisation void and incremental authorisation.	[0-9-]	1.12
z30	Indicates the Processor Routing Method used for the transaction. Optional values are: 1 Routing parameter (r1 or r2) 2 Routing rules 3 Processor priority	[0-9]	1,1

Name	Description	Type	Length
z31	The Processor Routing Rule ID that was responsible for the routing decision. Only populated in cases where z30=2.	[0-9]	0,4
z33	The Payment Processor processed the transaction.	[A-Z]	1,255
z34	The Payment Processor MID.	[a-zA-Z0-9]	1,255
z35	Indicates whether Smart Routing reroute is applied to this transaction.	Boolean	4,5
z36	The first Payment Processor to which the transaction was routed. Only populated in cases where all the following is true: • Smart Routing is enabled • The transaction was rerouted to a second processor • r1 was not sent on the request • The response did not contain certain z6 values	[A-Z]	1,255
z37	The original Response Code as transmitted by the first Payment Processor to which the transaction was routed (i.e., the z41 of the first Payment Processor to	[a-zA-Z0-9]	1,255

Name	Description	Type	Length
	which the transaction was routed). Only populated in cases where all the following is true: • Smart Routing is enabled • The transaction was rerouted to a second processor • r1 was not sent on the request • The response did not contain certain z6 values.		
z39	The Payment Processor Transaction ID. Used when corresponding with the Payment Processor or when reconciling transactions.	[a-zA-Z0-9]	1,255
z40	Fraud Explanation Array. Indicates the risk score and provides the list of rules that were triggered with respect to the transaction in question.	[a-zA-Z0-9]	5,4192
z41	The original Response Code as transmitted by the Processor. For more information, refer to Appendix D: Processing Response Reason Codes.	[a-zA-Z0-9]	1,255
z43	Indicates whether the transaction was handled by the Shift4 stand-in service as well as the transaction status. Possible values are:	[0-9]	1

Name	Description	Type	Length
	1 Transaction pending Shift4 stand-in service 2 Shift4 stand-in service final response 3 Transaction does not meet Shift4 stand-in max aggregated transaction amount threshold 4 Transaction does not meet Shift4 stand-in max transaction amount threshold 5 Unable to get final answer from the connector / processor. Shift4 stand-in service terminated for this transaction		
Z44	Merchant Advice Code (MAC) Indicates whether an attempt to retry the transaction is advised. Possible values: • 01: Updated or additional information needed • 02: Try again later • 03: Do not try again. **Note: This indicates a final decline** • 04: Token requirements not fulfilled for this token type • 21: Payment cancelation	[0-9]	2

Name	Description	Type	Length
	Note: This indicates a final decline • 22: Merchant does not qualify for product code • 24: Retry after 1 hour • 25: Retry after 24 hours • 26: Retry after 2 days • 27: Retry after 4 days • 28: Retry after 6 days • 29: Retry after 8 days • 30: Retry after 10 days • 40: Non-reloadable prepaid card 41: Consumer single-use virtual card number		
z50	Initial transaction ID. Received as part of the initial transaction response parameters. Must be sent for every subsequent 'merchant initiated transaction' in parameter g6 (see above).	[a-zA-Z0-9]	13,15
z51	Fast funds indicator. Indicates whether the issuer supports fast funds functionality. Y - Supports fast funds for domestic & cross-border payments	[A-Z]	1,1

Name	Description	Type	Length
	C - Supports fast funds for cross-border payments D - Supports fast funds for domestic payments N - No result		
z55	Payment ID. A unique transaction identifier that accompanies all transactions related to the same purchase.	[a-zA-Z0-9]	32,32
3ds_eci	The ECI assigned to the authentication	[0-9]	1,2
3ds_cavv	The authentication value received from the issuer	[a-zA-Z0-9]	0,64
3ds_trxid	The assigned 3D transaction ID	[a-zA-Z0-9]	36,36
3ds_xid	XID generated as part of the authentication. Relevant only for 3D Secure version 1.0.2	[a-zA-Z0-9]	28,28
3ds_status	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	[A-Z]	1,1

Name	Description	Type	Length
	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		
3ds_valid_payment	Shift4 recommendation whether to initiate payment following the authentication results. Possible values: y – yes n - no	Boolean	1,1
3ds_version	Indicates the 3D Secure protocol version Possible values: • 1.0 • 2.0 • 2.1.0 • 2.2.0	[0-9]	3,5

Name	Description	Type	Length
3ds_acsurl	The received issuer URL for the authentication process	[a-zA-Z0-9]	0,2048
3ds_pareq	Relevant only for 3D secure 1.0 flows. Used when accessing the 3ds_acsurl	[a-zA-Z0-9]	0,2048
3ds_acstrxid	Unique transaction identifier assigned by the ACS to identify a single 3D secure transaction.	[a-zA-Z0-9\-]	36,36
funding	This field has a value of "true" if the transaction is AFT. Otherwise, the field does not appear in the response.	True|False	4,5

Appendix A: Message Cipher

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

Calculating the Signature

The signature is calculated as follows:

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

Note:

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

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

Signature Calculation Example

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

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

1. Sort the parameters:

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

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

4. Line up the values:

   8632876178946541099454545454545454510811003John SmithAB1 2DEjohnsmith@yahoo.com111.222.0.101

5. Append the signature key exactly as it appears in your connectivity details:
6. 8632876178946541099454545454545454510811003John SmithAB1 2DEjohnsmith@yahoo.com111.222.0.101SIGNKEY1
7. Calculate the SHA256 hash of the sorted value set:
8. 8f03b86acd09da945e367e9f73151252cfc59a3c27ad8402bdd6e543c948232f
9. Include the signature into the request query string:
10. K=8f03b86acd09da945e367e9f73151252cfc59a3c27ad8402bdd6e543c948232f&M=8632876&O=1&a1=7894654&a4=1099&b1=4545454545454545&b2=1&b3=08&b4=11&b5=003&c1=John Smith&c10=AB1 2DE&c3=johnsmith@yahoo.com&d1=111.222.0.101

Note:

All API request strings should be URL encoded before being sent to the gateway as part of the HTTPS POST methods

Response Signature

If a request results in a successful transaction, the Shift4 Gateway will generate a response signature that can be validated in order to ensure the response's authenticity. In order to do so, apply the steps listed above to the response data and append your signature key (but remove the returned signature). We recommend that you check that both the generated signature and the response signature match.

Appendix B: Operation Result Codes

Here's a list of the possible result codes that may be returned in the z2 code:

Code	Description
-69	Transaction has been declined. Invalid 3ds_version parameter.
-68	Authentication process timed out. Please try again.
-66	Invalid combination of 3ds_initiate and exemption_action values
-65	Gateway MID is not allowed for this exemption
-64	TRA exemption is not allowed for this transaction amount
-63	The requested gateway mid is not enrolled to 3D-secure service.
-50	An error occurred during the 3D secure process
-39	You need to be registered with the 3D Adviser service to complete the request
-38	The transaction has been denied by the Gateway because 3D secure Authentication failed. Reason: {} **Note: The "Reason" part is optional and may appear according to detected reason.**
-37	Transaction has been denied. Malformed or missing {} parameter. Originating component: {}
-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.
-30	Transaction Failed due to error in 3D secure process
-20	Processor authentication error. Please contact Credorax support.
-17	Fraud-protection service is unavailable
-16	Rejected. Overriding the fraud threshold is not allowed
-15	Rejected. Bypassing the fraud service is not allowed.
-13	The requested gateway mid is not enrolled in the 3D Secure Adviser service.
-12	Transaction has been declined due to security restrictions.
-11	Rejected. Format Error
-10	Internal server error. Please contact *Shift4* support.
-9	The parameter is malformed.
-8	The Package Signature is malformed.

Code	Description
-7	Incorrect Gateway Response. Connection is broken.
0	The transaction has been executed successfully.
1	The transaction has been denied by the Gateway.
2	The transaction has been denied by the Gateway due to its high fraud risk.
03	The transaction has been denied by the Gateway due to its high AVS risk.
04	The transaction has been denied by the Gateway due to an interchange timeout.
05	The transaction has been declined.
06	Transaction pending cardholder authentication.
07	The transaction was declined by the gateway and will not be processed due to retry optimization policy.
9	The transaction has been denied by the Gateway due to a LUHN check failure
10	The transaction has been partially approved.
11	The queried transaction is currently being processed. Please try again.
13	Rejected. The fraud-protection service is unavailable.
15	Rejected. Risk score is above limit.

Appendix C: AVS Response Codes

AVS Authorisation responses provided by the issuer at the time of Authorisation.

In the case of 2-character response codes, the AVS verification response code is the second character of the value returned by the z9 field.

A response code of "-", "E", "S", "U" or "I" indicates the AVS service is not available for the particular card. The response code "R" indicates that the issuer was not available and that the operation should be retried later.

Code	Description
A	Partial Match - Address match; ZIP/Postal Code does not match
B	Partial Match - Address match; ZIP/Postal Code not supplied or not checked
C	No Match – Address and ZIP/Postal Code not verified
D	Full Match - Address and ZIP/Postal Code match
E	Invalid: AVS data is invalid or AVS is not allowed for this card type.
F	Full Match - Address and ZIP/Postal Code match (UK Only)
G	No Match - Address not verified
H	Partial match: Cardholder's Name does not match, but Street Address and Postal Code do. Only returned for the American Express card type.
I	Address not verified
K	Partial match: Cardholder's Name matches, but Billing Address and Billing Postal Code do not match. Returned only for the American Express card type.
L	Partial match: Cardholder's Name and Billing Postal Code match, but Billing Address does not match. Returned only for the American Express card type.
M	Full Match - Address and ZIP/Postal Code match
N	No Match - Address and ZIP/Postal Code do not match
O	Partial match: Cardholder's Name and Billing Address match, but Billing Postal Code does not match. Returned only for the American Express card type.
P	Partial Match - ZIP/Postal Code matches but Address does not
R	Issuer system unavailable or timeout. Retry.
S	AVS not supported by issuer
T	Partial match: Cardholder's Name does not match, but Street Address does. Returned only for the American Express card type.
U	Address information unavailable

Code	Description
V	Match: Cardholder's Name, Billing Address, and Billing Postal Code match. Returned only for the American Express card type.
W	For US addresses: Partial Match - Nine-digit ZIP Code matches, but Address does not match. For addresses outside the US: Partial Match - Postal Code matches but Address does not
X	For US addresses: Full Match - Nine-digit ZIP Code and Address match
Y	Full Match - Five-digit ZIP Code and Address match
Z	Partial Match – Five-digit ZIP Code matches, but Address does not

The following table provides another view of the possible Response Codes grouped by Postal/ZIP Code/Area Type: U.S. 5-digit ZIP code, International address, U.S. ZIP+4 , no ZIP code, and no address.

Table 2:

Type	Full match	Partial match	No match
U.S. 5-digit ZIP Code	F, Y	A	N
International address	M	P	G
U.S. ZIP+4	X	W	N/A
No ZIP code	N/A	B	D
No address	N/A	Z	C

Appendix D: Processing Response Reason Codes

The following table lists the possible response codes returned in the z6 parameter. Note that this value is not generated by the Shift4 payment gateway. Your system should support receiving other values than the ones listed below.

Code	Description
00	Approved or completed successfully
01	Refer to card issuer
02	Refer to card issuer - special condition
03	Invalid merchant
04	Pick up card
05	Do not honour
06	Error
07	Pick up card - special condition
08	Honour with identification
10	Partial amount approved
12	Invalid transaction
13	Invalid amount
14	Invalid card number
15	No such issuer
19	Re-enter transaction
21	No action taken
30	Format error
34	Implausible card data
39	No credit account
41	Lost card, pick up
42	No universal account
43	Pick up, stolen card
44	No investment account
46	Closed account
50	Do not renew
51	Insufficient funds

Code	Description
52	No checking account
53	No savings account
54	Expired card
55	Incorrect PIN
57	Transaction not allowed for cardholder
58	Transaction not permitted to terminal
59	Suspected fraud
61	Exceeds withdrawal limit
62	Restricted card
63	Security violation
64	Wrong original amount
65	Activity count limit exceeded
68	Response received too late
70	PIN data required
71	Decline, PIN not changed
75	PIN tries exceeded
76	Wrong PIN, number of PIN tries exceeded
77	Wrong Reference Number
78	Blocked, first used/ Record not found
79	Declined due to lifecycle event
80	Network error
81	PIN cryptographic error
82	Bad CVV/ Declined due to policy event
83	Transaction failed
84	Pre-authorization timed out
85	No reason to decline
86	Cannot verify PIN
87	Purchase amount only, no cashback allowed
88	Cryptographic failure
89	Authentication Failure

Code	Description
91	Issuer not available
92	Unable to route at acquirer module
93	Transaction cannot be completed, violation of law
94	Duplicate transmission
95	Reconcile error / Auth not found
96	System malfunction
97	Transaction has been declined by the processor
N3	Cash service not available
N4	Cash request exceeds issuer or approved limit
N7	CVV2 failure
R0	Stop Payment Order
R1	Revocation of Authorisation Order
R3	Revocation of all Authorisation Orders
1A	Strong Customer Authentication required

Appendix E: z21 Possible Values

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

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

Appendix F: Additional Request Parameters

The following parameters can be used to support specific business scenarios, according to your preferences or the industry you operate in.

User Device Information

Name	Type	Min	Max	Description
d5	[a-zA-Z0-9\:\=\+]	5	255	The browser's user agent header
d6	[a-zA-Z,-]	2	16	Accept-Language header, comma-separated set of locales
d8	[a-zA-Z0-9]	1	64	Browser version
d9	[a-zA-Z0-9]	1	64	Device type (mobile, tablet, iPad, desktop, etc.)
d10	[a-zA-Z0-9]	1	64	Device Operating System name
d11	[a-zA-Z0-9]	1	64	Device Operating System version

Retail

Name	Type	Min	Max	Description
re1	[0-9]	1	10	Number of items purchased
re2	[a-zA-Z0-9]	1	64	Purchase Invoice Number
re3	[a-zA-Z0-9]	1	64	Shipping Class (Regular, VIP, Express, etc.)
re4	DATE	1	10	Expected Delivery Date (YYYYMMDD)
re5	[a-zA-Z0-9]	1	64	Purchase Discount Code

Gaming

Name	Type	Min	Max	Description
ga1	[0-9]	1	16	Account Balance
ga2	[a-zA-Z0-9]	1	64	Game ID
ga3	[a-zA-Z0-9]	1	64	Game Name
ga4	[a-zA-Z0-9]	1	64	Time in Game (in seconds)
fo1	[a-zA-Z0-9]	1	9	Traded Currencies (XXX, YYY) Format

Name	Type	Min	Max	Description
st1	[a-zA-Z0-9]	1	64	Movie Name or Series Name
st2	[a-zA-Z0-9]	1	64	Movie or Series ID

Forex

Name	Type	Min	Max	Description
fo1	[a-zA-Z0-9]	1	9	Traded currencies (XXX, YYY) format

Streaming

Name	Type	Min	Max	Description
st1	[a-zA-Z0-9]	1	64	Movie name or series name
st2	[a-zA-Z0-9]	1	64	Movie or series ID

Amount Components

Name	Type	Min	Max	Description
a41	[0-9]	1	12	Subtotal amount
a42	[0-9]	1	12	VAT amount
a44	[0-9]	1	12	Shipping amount
a46	[0-9]	1	12	Tip amount

Furniture

Name	Type	Min	Max	Description
fu1	[a-zA-Z0-9]	1	50	The furniture supplier name

Car, Plane and Boat Rentals

Name	Type	Min	Max	Description
cr1	[a-zA-Z0-9]	1	50	The supplier/contractor name

Event Management

Name	Type	Min	Max	Description
ev1	YYYYMMDD	10	10	Event start date
ev2	YYYYMMDD	10	10	Event end date
ev3	[a-zA-Z0-9]	1	50	Event organizer ID
ev4	[a-zA-Z0-9]	1	50	Event ID

Travel

The Travel parameters enable the merchant to provide more ticket information on the transaction itself, enabling cardholders to properly identify non-ticket related passenger transport service charges, leading to reduced transaction disputes and chargebacks.

Travel parameters are relevant only for Travel Agency and Airlines MCCs.

Name	Type	Min	Max	Description
ota1	[a-zA-Z0-9]	1	64	Ticket number
ota2	[a-zA-Z0-9]	1	64	Travel agency code
ota3	[a-zA-Z0-9]	1	64	Passenger name
ota5	[a-zA-Z0-9]	1	64	Travel agency
ota6	[a-zA-Z0-9]	3	128	E-ticket email address
ota7	[a-zA-Z0-9]	1	64	Airline name
ota12	[a-zA-Z0-9]	1	64	Frequent Flier Number
ota14	[a-zA-Z0-9]	1	1	Restricted Ticket Indicator. Indicates whether this ticket is non-refundable. Possible values: 0 - No restriction 1 – Restricted
ota15	[a-zA-Z0-9]	1	4	Computer Reservation System. Indicates the computerised reservation system used to make the reservation and purchase the ticket.
ota16	[a-zA-Z0-9]	1	1	Refund Reason Indicator. Indicates the reason for a cardholder refund. Possible values: A – Passenger Transport Ancillary Purchase Cancellation B – Airline Ticket and Passenger Transport Ancillary Purchase Cancellation O – Other

<table>
<tr><th>Name</th><th>Type</th><th>Min</th><th>Max</th><th>Description</th></tr>
<tr><td>ota17</td><td>[a-zA-Z0-9]</td><td>1</td><td>1</td><td>Ticket Change Indicator. Indicates why a ticket was changed. Values are:
C - Change to existing ticket
N - New ticket</td></tr>
<tr><td>ota18</td><td>[a-zA-Z0-9]</td><td>1</td><td>13</td><td>Issued in Connection with Ticket Number. If this purchase has a connection to or a relationship with another purchase, such as a baggage fee for a passenger transport ticket, this field should contain the ticket document number for the other purchase.
For a stand-alone purchase where this field is mandatory, the field must contain the same value as the value in the Ancillary Ticket Document Number field.</td></tr>
<tr><td>ota19</td><td>[a-zA-Z0-9]</td><td>1</td><td>15</td><td>Ancillary Ticket Document Number.
Contains the form number assigned by the carrier for the transaction.</td></tr>
<tr><td>ota20</td><td>[a-zA-Z0-9]</td><td>1</td><td>6</td><td>The airline code</td></tr>
<tr><td>ota21</td><td>[a-zA-Z0-9]</td><td>1</td><td>50</td><td>The contractor name</td></tr>
<tr><td>ota22</td><td>[a-zA-Z0-9]</td><td>1</td><td>255</td><td>ATOL certificate number</td></tr>
<tr><td>fl1</td><td>[a-zA-Z0-9\:\-]</td><td>9</td><td>48</td><td>First flight information. This field contains the following flight information, delimited by “:”:
<table>
<tr><th>Field</th><th>Type</th><th>min</th><th>max</th></tr>
<tr><td>Travel Date</td><td>YYYY-MM-DD</td><td>0</td><td>10</td></tr>
<tr><td>Carrier Code</td><td>[a-zA-Z0-9]</td><td>0</td><td>2</td></tr>
<tr><td>Service Class</td><td>[a-zA-Z0-9]</td><td>0</td><td>1</td></tr>
<tr><td>City of Origin</td><td>[a-zA-Z0-9]</td><td>0</td><td>3</td></tr>
<tr><td>Destination City</td><td>[a-zA-Z0-9]</td><td>0</td><td>3</td></tr>
<tr><td>Stopover Indicator</td><td>[a-zA-Z0-9]</td><td>0</td><td>1</td></tr>
<tr><td>Fare Basis Code</td><td>[a-zA-Z0-9]</td><td>0</td><td>6</td></tr>
<tr><td>Flight Number</td><td>[a-zA-Z0-9]</td><td>0</td><td>5</td></tr>
<tr><td>Originating Airport Code</td><td>[a-zA-Z0-9]</td><td>0</td><td>5</td></tr>
</table></td></tr>
</table>

Name	Type	Min	Max	Description
				Flight's Fare [a-zA-Z0-9] 0 12
fl2	[a-zA-Z0-9\:]	9	48	Second flight information. Same format as fl1
fl3	[a-zA-Z0-9\:]	9	48	Third flight information. Same format as fl1
fl4	[a-zA-Z0-9\:]	9	48	Fourth flight information. Same format as fl1
fl5	YYYYMMDD	8	8	Flight departure date
fl6	YYYYMMDD	8	8	Flight arrival date
an1	[a-zA-Z0-9\:\-]	8	38	First ancillary information. This field contains the following ancillary information delimited by ":" (refer to Appendix K: Ancillary Fee Codes for more information). **Field** **Type** **min** **max** Ancillary Fee Code [a-zA-Z0-9] 0 4 Ancillary Fee Amount [a-zA-Z0-9] 0 12 Ancillary Fee Code Sub-Category [a-zA-Z0-9] 0 4
an2	[a-zA-Z0-9\:]	8	38	Second ancillary information. Same format as an1. Refer to Appendix K: Ancillary Fee Codes for more information.
an3	[a-zA-Z0-9\:]	8	38	Third ancillary information. Same format as an1. Refer to Appendix K: Ancillary Fee Codes for more information.
an4	[a-zA-Z0-9\:]	8	38	Fourth ancillary information. Same format as an1. Refer to Appendix K: Ancillary Fee Codes for more information.

Customer Identity

Name	Type	Min	Max	Description
c12	[a-zA-Z0-9]	1	32	Customer Level (VIP, Basic)
c13	[a-zA-Z0-9]	1	32	Customer ID (Shopper or Player ID)
c14	DATE	8	8	Customer Creation Date (YYYYMMDD)

Name	Type	Min	Max	Description
c15	DATE	8	8	Customer Date of Birth (YYYYMMDD)
c16	[a-zA-Z0-9]	1	32	Customer Username
c17	[a-zA-Z0-9]	3	255	Customer User Email
C18	[a-zA-Z0-9]	1	32	ID / Passport number

Appendix G: r1 Possible Values

A list of possible values for the r1 request parameter:

#	Value
1	CREDORAX
2	Nuvei
3	ISRACARD
4	MAX
5	CAL
6	NBK
7	AMEX
8	Raiffeisen
9	BNP
10	Worldpay

Appendix H: Transaction Currencies

The following table contains a list of currencies that are currently supported by the *Shift4* Payment Gateway. These values should be transmitted via the a5 parameter and indicate the transaction currency that should be used for the transaction.

Note:

- For currencies with two exponents the two right most digits are considered the exponents (for example, if you want to process a transaction of GBP 10.00 you should send the amount value as a4=1000
- For currencies with three exponents
  - the three right most digits of the amount are considered the exponents. For example, to process a transaction of KWD 10.000 you should send the amount value as a4=10000
  - For Visa transactions, the last digit of the amount in a 3-exponent currency must be zero (0). Transmitting a 3-exponents transaction in any other format may result in a decline.
- For currencies with zero exponents you should send the exact amount values. For example, to process a transaction of JPY 10 you should send the amount value as a4=10
- Some processors may decline a transaction in a currency that was not authorized for your account. Refer to the Shift4 Global Processors Specifications to learn more about the currencies supported by each processor

Country	Currency	Currency Code	Exponent
United Arab Emirates	United Arab Emirates Dirham	AED	2
Afghanistan	Afghani	AFN	2
Albania	Lek	ALL	2
Armenia	Armenian Dram	AMD	2
Netherlands Antilles	Netherlands Antillean Guilder	ANG	2
Angola	Kwanza	AOA	2
Argentina	Argentine Peso	ARS	2
Australia	Australian Dollar	AUD	2
Aruba	Aruban Guilder	AWG	2
Azerbaijan	Azerbaijanian Manat	AZN	2

Country	Currency	Currency Code	Exponent
Bosnia Herzegovina	Convertible Marks	BAM	2
Barbados	Barbados Dollar	BBD	2
Bangladesh	Bangladeshi Taka	BDT	2
Bulgaria	Bulgarian Lev	BGN	2
Bahrain	Bahraini Dinar	BHD	3
Burundi	Burundian Franc	BIF	0
Bermuda	Bermuda	BMD	2
Brunei Darussalam	Brunei Dollar	BND	2
Bolivia	Boliviano	BOB	2
Brazil	Brazilian Real	BRL	2
Bahamas	Bahamian Dollar	BSD	2
Bhutan	Ngultrum	BTN	2
Botswana	Pula	BWP	2
Belarus	New Belarusian Ruble	BYN	2
Belize	Belize Dollar	BZD	2
Canada	Canadian Dollar	CAD	2
Congo, The Democratic Republic of	Franc Congolais	CDF	2
Switzerland	Swiss Franc	CHF	2
Chile	Chilean Peso	CLP	0
China	Chinese Yuan	CNY	2
Colombia	Colombian Peso	COP	2
Costa Rica	Costa Rican Colon	CRC	2
Cape Verde	Cape Verde Escudo	CVE	2
Czech Republic	Czech Koruna	CZK	2
Djibouti	Djibouti Franc	DJF	0
Denmark	Danish Krone	DKK	2
Dominican Republic	Dominican Peso	DOP	2
Algeria	Algerian Dinar	DZD	2
Egypt	Egyptian Pound	EGP	2

Country	Currency	Currency Code	Exponent
Eritrea	Nakfa	ERN	2
Ethiopia	Ethiopian Birr	ETB	2
19 European Union Countries (EMU)	Euro	EUR	2
Fiji	Fiji Dollar	FJD	2
Falkland Islands (Malvinas)	Falkland Islands Pound	FKP	2
United Kingdom	Pounds Sterling	GBP	2
Georgia	Lari	GEL	2
Ghana	Cedi	GHS	2
Gibraltar	Gibraltar Pound	GIP	2
Gambia	Dalasi	GMD	2
Guinea	Guinea Franc	GNF	0
Guatemala	Quetzal	GTQ	2
Guyana	Guyana Dollar	GYD	2
Hong Kong	Hong Kong Dollars	HKD	2
Honduras	Lempira	HNL	2
Haiti	Haitian Gourde	HTG	2
Hungary	Forint	HUF	2
Indonesia	Rupiah	IDR	2
Israel	Israeli New Sheqel	ILS	2
India	Indian Rupee	INR	2
Iraq	Iraqi Dinar	IQD	3
Iceland	Iceland Krona	ISK	0
Jamaica	Jamaican Dollar	JMD	2
Jordan	Jordanian Dinar	JOD	3
Japan	Japanese Yen	JPY	0
Kenya	Kenyan Shilling	KES	2
Kyrgyzstan	Som	KGS	2
Cambodia	Riel	KHR	2
Comoros	Comoro Franc	KMF	0

Country	Currency	Currency Code	Exponent
Korea, Republic of	South Korean Won	KRW	0
Kuwait	Kuwaiti Dinar	KWD	3
Cayman Islands	Cayman Islands Dollar	KYD	2
Kazakhstan	Tenge	KZT	2
Lao People's Democratic Republic	Kip	LAK	2
Lebanon	Lebanese Pound	LBP	2
Sri Lanka	Sri Lanka Rupee	LKR	2
Liberia	Liberian Dollar	LRD	2
Lesotho	Lesotho Loti	LSL	2
Libyan Arab Jamahiriya	Libyan Dinar	LYD	3
Morocco	Moroccan Dirham	MAD	2
Moldova, Republic of	Moldovan Leu	MDL	2
Madagascar	Malagasy Ariary	MGA	2
Macedonia	Denar	MKD	2
Myanmar	Kyat	MMK	2
Mongolia	Tugrik	MNT	2
Macao	Pataca	MOP	2
Mauritania	Mauritania	MRU	2
Mauritius	Mauritius Rupee	MUR	2
Maldives	Rufiyaa	MVR	2
Malawi	Kwacha	MWK	2
Mexico	Mexican Peso	MXN	2
Malaysia	Malaysian Ringgit	MYR	2
Mozambique	Metical	MZN	2
Namibia	Namibian Dollar	NAD	2
Nigeria	Naira	NGN	2
Nicaragua	Cordoba Oro	NIO	2
Norway	Norwegian Krone	NOK	2
Nepal	Nepalese Rupee	NPR	2

Country	Currency	Currency Code	Exponent
New Zealand	New Zealand Dollar	NZD	2
Oman	Omani Rial	OMR	3
Panama	Balboa	PAB	2
Peru	Nuevo Sol	PEN	2
Independent State of Papua New Guinea	Kina	PGK	2
Philippines	Philippine Peso	PHP	2
Pakistan	Pakistani Rupee	PKR	2
Poland	Zloty	PLN	2
Paraguay	Guarani	PYG	0
Qatar	Qatari Rial	QAR	2
Romania	Romanian New Leu	RON	2
Serbia	Serbian Dinar	RSD	2
Russia	Russian Rouble	RUB	2
Rwanda	Rwanda Franc	RWF	0
Saudi Arabia	Saudi Riyal	SAR	2
Solomon Islands	Solomon Islands Dollar	SBD	2
Seychelles	Seychelles Rupees	SCR	2
Sweden	Swedish Krona/Kronor	SEK	2
Singapore	Singapore Dollar	SGD	2
Saint Helena, Ascension and Tristan Da Cunha	Saint Helena Pound	SHP	2
Sierra Leone	Leone	SLE	2
Somalia, Federal Republic of	Somali Shilling	SOS	2
Suriname	Surinam Dollar	SRD	2
South Sudan	South Sudanese Pound	SSP	2
Sao Tome and Principe	Sao Tome Principe	STN	2
El Salvador	El Salvador Colon	SVC	2
Syrian Arab Republic	Syrian Pound	SYP	2
Swaziland	Lilangeni	SZL	2

Country	Currency	Currency Code	Exponent
Thailand	Baht	THB	2
Tajikistan	Somoni	TJS	2
Turkmenistan	Manat	TMT	2
Tunisia	Tunisian Dinar	TND	3
Tonga	Paanga	TOP	2
Turkey	Turkish Lira	TRY	2
Trinidad And Tobago	Trinidad and Tobago Dollar	TTD	2
Taiwan Province of China	New Taiwan Dollar	TWD	2
Tanzania, United Republic of	Tanzanian Shilling	TZS	2
Ukraine	Hryvnia	UAH	2
Uganda	Uganda Shilling	UGX	2
United States	US Dollar	USD	2
Uruguay	Peso Uruguayo	UYU	2
Uzbekistan	Uzbekistan Som	UZS	2
Venezuela	Venezuelan Bolívar Fuerte	VES	2
Vietnam	Vietnamese Dông	VND	0
Vanuatu	Vatu	VUV	0
Samoa	Samoan Tala	WST	2
Central African Republic	CFA Franc BEAC	XAF	0
Eastern Caribbean States	East Caribbean Dollar	XCD	2
Communauté Financière Africaine	CFA Franc BCEAO	XOF	0
French Polynesia	CFP Franc	XPF	0
Yemen	Yemeni Rial	YER	2
South Africa	South African Rand	ZAR	2
Zambia	Kwacha	ZMW	2
Zimbabwe	Fourth Zimbabwe Dollar	ZWL	2

Appendix I: 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 J: How to provide 3D secure information on i8 parameter.

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 version of the 3D Secure protocol: 3D Secure 1.0, 2.0, 2.1.0 and 2.2.0
- To use Shift4's 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 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.

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 transaction.
- 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 you 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 '3ds_initiate' parameter as part of the payment request (applicable for operations: Sale, Authorisation and CFT of all types).

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

Value	Description
01	Initiate 3D Secure before completing the payment
02	Process payment without 3D Secure
03	Initiate 3D Secure according to the 3DS Adviser result (see 3DS Adviser)
04	Only initiate the 3DS Adviser service. Relevant only for op code 98

Note:

- The transaction will only be processed if the 3D secure process is completed successfully, whether in a frictionless flow or a challenge flow.
- When initiating the 3DS Adviser, if the decision engine determines the transaction should go through 3D Secure, 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]. Refer to the Special Operations section for more details

Standard 3D Secure Workflow

When 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:

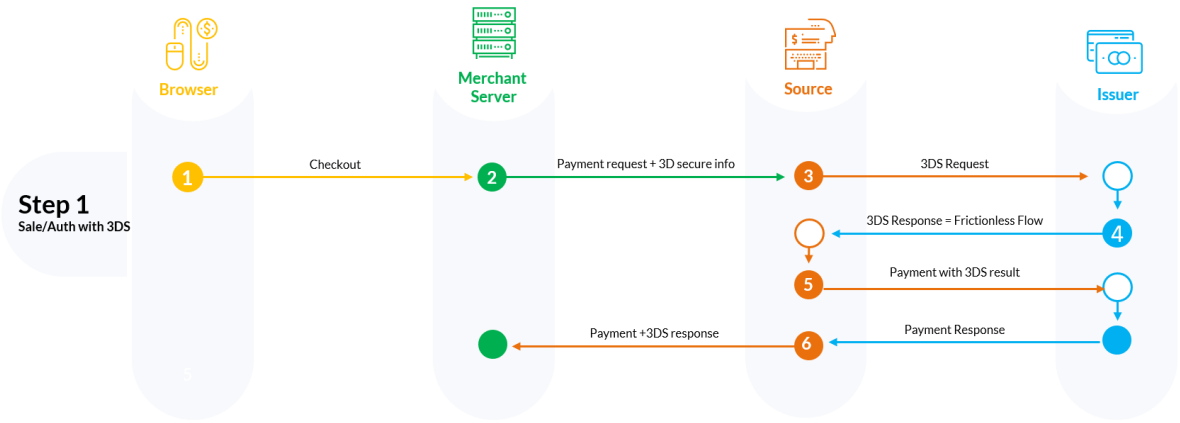
Entity	Description
Browser	The cardholder's browser from which the process was initiated
Merchant Server	The merchant's server side
Shift4	Shift4 Payment Gateway
Issuer	The issuer of the card used in the transaction

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.

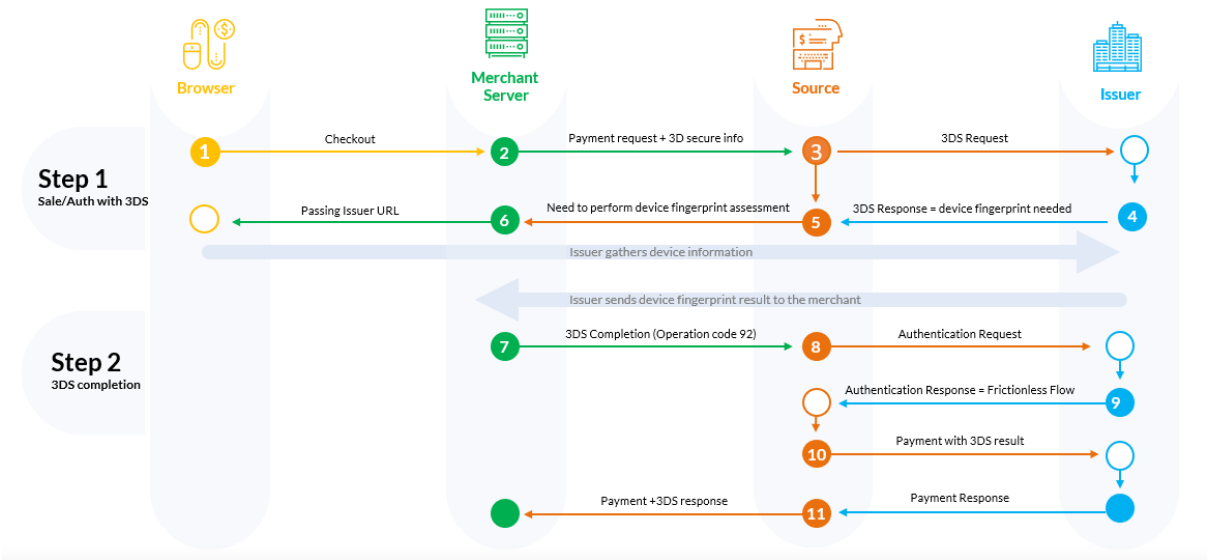
Steps 3-4: Shift4 initiates the 3D secure authentication process and receives a response from the issuer that no further authentication is required

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

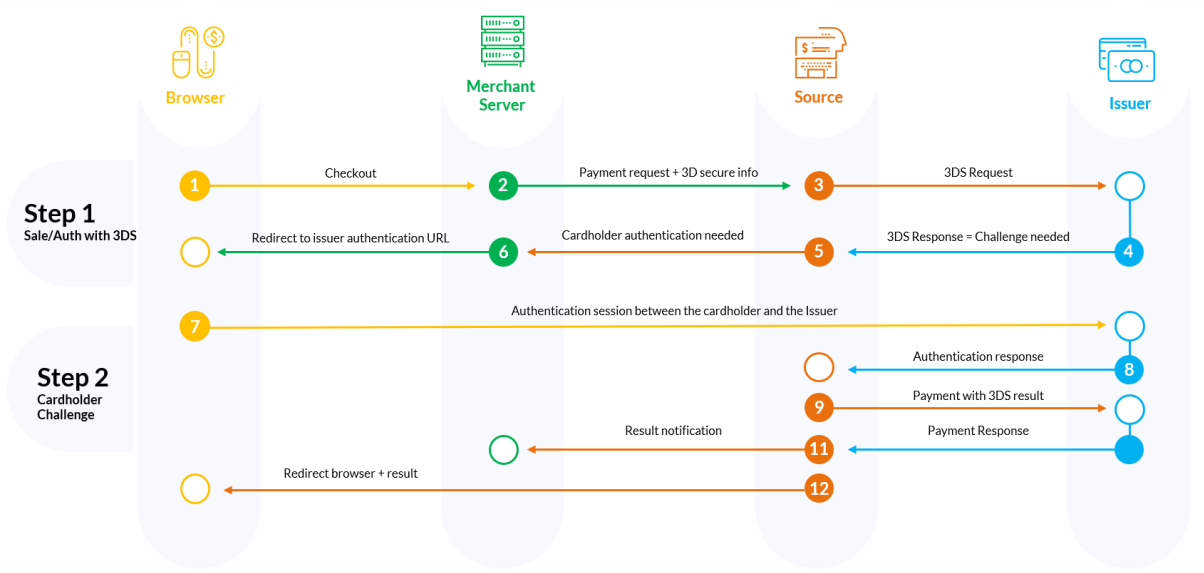
Steps 8-9: Shift4 re-initiates the 3D secure authentication process with the input received through operation code [92], and receives the authentication result from the issuer

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.

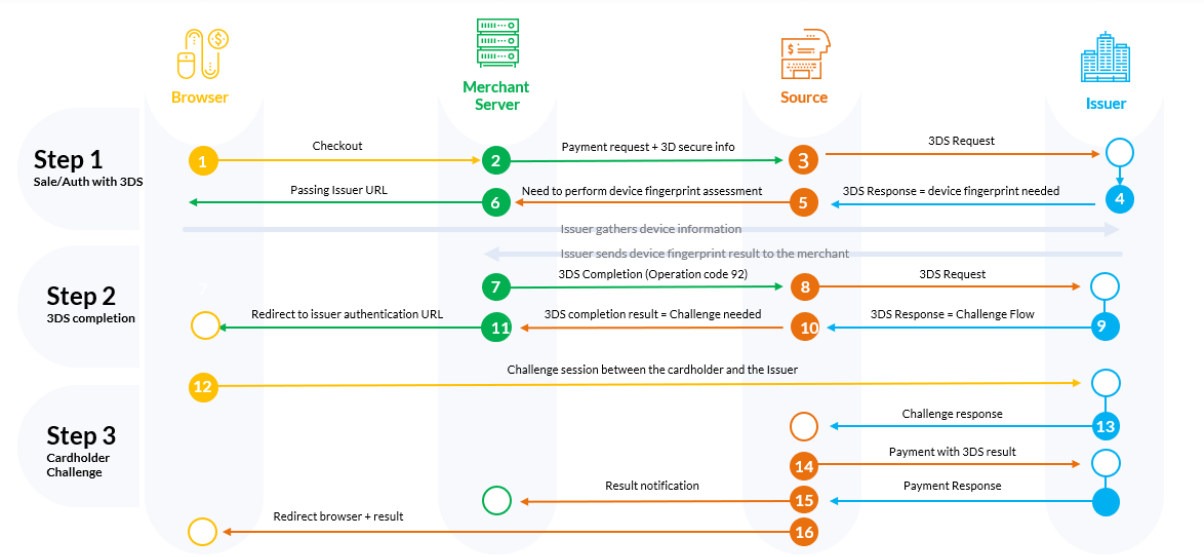
Step 10: Shift4 initiates the payment

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 operation code [92], 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
3ds_method	URL	The issuer's URL that should be used to trigger the collection of the device fingerprint by the issuer
3ds_trxid	[a-zA-Z0-9, -]	Universally unique transaction identifier to identify a single 3DS transaction.

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

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

threeDSServerTransID = <3ds_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 3DS_Method 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 contain a single encoded parameter called threeDSMethodData.

   Note: If the notification is received within 10 seconds, then when executing step , set 3ds_copmind = Y; otherwise, set 3ds_compind = N.
5. Use the information from the response to send a completion call to Shift4. This is done by sending operation code [92] in the following structure:

Name	Description	Type	Length	Completion Operation [92]
M	Shift4 assigned gateway Merchant ID	[A-Z0-9_]	3,6	m
K	Unique cipher used for authenticating requests Refer to Appendix A: Message Cipher for further details on generating the cipher.	[0-9A-Za-z]	1,32	m
O	Operation Code The operation code is used to determine the requested service.	[0-9]	1,3	m

Name	Description	Type	Length	Completion Operation [92]
a1	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. Note: No plaintext cardholder data should be provided in this field.	[A-Za-z0-9-]	1,32	m
g5	Referred transaction ID. Populate this field with the received z1 of the original transaction.	[0-9]		m
3ds_trxid	Universally unique transaction identifier to identify a single 3DS transaction.	[a-zA-Z0-9, -]	36,36	m
3ds_compind	Received from the issuer. Indicates whether the device fingerprint collection completed successfully.	[Y, N]	1,1	m

Cardholder challenge flow

Whenever a cardholder challenge is required, you have to redirect the browser to the Issuer's side in order to allow the authentication process between the issuer the cardholder.

You will receive a 3ds_acsurl parameter as part of the original payment request or as the response to operation code [92] (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 3ds_acsurl parameter. However, for a 3DS 1.0 protocol, it is recommended to redirect to the address received in the 3ds_acsurl 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
f23	[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
smart_3ds_result	[0-4]	2	2	Describes the 3DS Adviser module recommendation: 01: Do 3D secure 02: Skip 3D secure 03: Request an exemption as part of the 3D Secure request 04: Request an exemption as part of the payment request
smart_3ds_result_reason	[a-zA-Z0-9]	0	128	Includes the rule id which was executed as part of the Smart 3D rule engine

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
exemption_action	[0-9]	o	2,2	Indicates the merchant preference regarding SCA exemption. Possible values are: 01: Do not request exemption. This is the default behavior for the Shift4 Gateway. If the field is absent from the transaction request, no exemption will be applied. 02: Request an exemption as part of the payment request. 03: Request an exemption as part of the 3D Secure request 04: Request exemption by default. Shift4 will apply for exemption as part of the 3D Secure request if possible. Note: If no value is provided, and you are using the 3DS Adviser module, the Shift4 Payment Gateway requests an exemption (if applicable) as part of the 3D secure process.
exemption_reason	[0-9]	o	2,2	This field is required when exemption_action = 02 or 03. Possible values: 01: Low value transaction (below 30 EUR or equivalent) 02: Low risk transaction (TRA)1 03:Request Trusted Beneficiary Indicator (Whitelisting)2 04: Secure Corporate Cards 3 05: Delegated Authentication 4 06: MIT – Recurring same amount 07: MIT – other 5 08: Trusted Beneficiary Indicator (Whitelisting) – Done6 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

Name	Type	o/m	Min, Max	Description
				3 This is not a standard exemption you can request. If you know the card used for the transaction is a secure corporate card, use this value to indicate so to Shift4. This will help the 3DS Adviser determine the optimal 3D Secure employment. 4 This exemption option can be used if you implemented an alternative SCA solution as part of your checkout process. This requires your solution be pre-approved and registered with the card schemes. 5 Any MIT transaction must be sent with this flag to make sure the transaction will not require SCA. 6 This is not a standard exemption you can request. If you receive an indication you were whitelisted by a cardholder, use this value on any subsequent transaction by that cardholder to indicate back to the Shift4 gateway that this is a potential whitelisting card. This will help the 3DS Adviser determine the optimal 3D Secure employment.
tra_score	[0-9,A-Za-z]	c	1,8	Indicates the transaction risk analysis result calculated by a third party provider as a basis for exemption_reason=02

Managing SCA for Merchant initiated transaction

Merchant initiated transactions can occur in two business cases:

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

Exemption – Response Parameters

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

3D Secure Authentication-Only Flow

You may choose to use the Shift4 Payment Gateway 3D Secure Service without completing the transaction processing through the Shift4 Payment Gateway. To do so, use operation [98]. Alternatively, use either operation [88] which first creates a token, or operation [89] which uses a token, and then initiate a 3D Secure authentication-only flow.

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 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

Requested Data	Shift4 Parameters	Description
	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
	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_initate=01 or 03):

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

Name	Description	Type	min	max	m/o/c
3ds_sdkuitype	Contains a list of all UI types that the device supports for displaying specific challenge user interfaces within the SDK. Accepted values for each UI type are: 01 - Text 02 - Single select 03 - Multi select 04 - OOB 05 - Html Other (valid only for HTML UI) For Native UI SDK Interface accepted values are 01-04 and for HTML UI accepted values are 01-05.	Comma separated list	2	14	c m only when 3ds_channel=01 (APP).
3ds_reqauthmethod	Information about how the cardholder was authenticated before or during the transaction. The mechanism used by the Cardholder to authenticate to the merchant. Accepted values are: 01 - No authentication occurred (i.e., cardholder "logged in" as guest) 02 - Login to the cardholder account at the merchant system using merchant's own credentials 03 - Login to the cardholder account at the merchant system using federated ID 04 - Login to the cardholder account at the merchant system using issuer credentials 05 - Login to the cardholder account at the merchant system using third-party authentication 06 - Login to the cardholder account at the merchant system using FIDO Authenticator	[0-6]	2	2	o

Name	Description	Type	min	max	m/o/c
	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)				
3ds_reqauthtimestamp	Date and time in UTC of the cardholder authentication. Field is limited to 12 characters and the accepted format is YYYYMMDDHHMM	[0-9]	12	12	o
3ds_reqauthdata	Data that documents and supports a specific authentication process. The intention is that for each merchant Authentication Method, this field contains data that the issuer can use to verify the authentication process.	[a-zA-Z0-9]	0	255	o
3ds_reqchallengeind	Indicates whether a challenge is requested for this transaction. For example: For 3ds_category 01-PA, a merchant may have concerns about the transaction, and request a challenge. For 3ds_category 02-NPA, a challenge may be necessary when adding a new card to a wallet. 01 - No preference 02 - No challenge requested 03 - Challenge requested by merchant 04 - Challenge requested: Mandate 05 - No Challenge Requested, transactional risk analysis is already performed 06 - No Challenge Requested, Data share only	[0-4]	2	2	o

Name	Description	Type	min	max	m/o/c
	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)				
3ds_reqpriorref	This data element provides additional information to the issuer to determine the best approach for handling a request. The element contains the issuer's Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the cardholder).	[a-zA-Z0-9]	36	36	o
3ds_reqpriorauthmethod	Mechanism used by the Cardholder to previously authenticate to the merchant. Accepted values for this field are: 01- Frictionless authentication occurred by issuer 02 - Cardholder challenge occurred by issuer 03 - AVS verified 04 - Other issuer methods	[0-4]	2	2	o
3ds_reqpriorauthtimestamp	Date and time in UTC of the prior authentication. Accepted date format is YYYYMMDDHHMM.	[0-9]	12	12	0
3ds_reqpriorauthdata	Data that documents and supports a specific authentication process. In the current version of the specification this data element is not defined in detail, however the intention is that for each merchant Authentication Method, this field carry data that the issuer can use	[a-zA-Z0-9]	0	255	o

Name	Description	Type	min	max	m/o/c
	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.				
3ds_reqdecreqind	Indicates whether the merchant requests the ACS to utilise Decoupled Authentication and agrees to utilise Decoupled Authentication if the ACS confirms its use. Accepted values are: Y - Decoupled Authentication is supported and preferred if challenge is necessary N - Do not use Decoupled Authentication.	[Y,N]	1	1	o
3ds_reqdecmaxtime	Indicates the maximum amount of time (in minutes) that the merchant will wait for an ACS to provide the results of a Decoupled Authentication transaction. Valid values are between 1 and 10080.	[0-9]	1	5	o
3ds_chaccdate	Date that the cardholder opened the account with the merchant. Date format = YYYYMMDD.	[0-9]	8	8	o
3ds_chaccchangeind	Length of time since the cardholder's account information with the merchant was last changed. Includes Billing or Shipping address, new payment account, or new user(s) added. Accepted values are: 01 - Changed during this transaction 02 - Less than 30 days 03 - 30 - 60 days 04 - More than 60 days	[0-4]	2	2	o

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

Name	Description	Type	min	max	m/o/c
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
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_paymentacind	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

Name	Description	Type	min	max	m/o/c
3ds_paymentacage	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: – true -Merchant is whitelisted by cardholder – false - Merchant is not whitelisted by cardholder	[] [a-z]	4	5	o
3ds_paytokenind	This field has a value of "true" if the transaction was de-tokenised prior to being received by Shift4.	[a-z]	4	5	o
3ds_addrmatch	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical. Accepted values: • True - Shipping Address matches Billing Address • False - Shipping Address does not match Billing Address Note: the default value of this field is 'false'	[a-z]	4	5	o
3ds_homephonecountry	Country Code of the home phone.	[0-9]	1	3	o (m if c2 exists)
3ds_chmobilephone	The mobile phone provided by the Cardholder, without the country code	[0-9]	0	18	o
3ds_mobilephonecountry	Country Code of the mobile phone.	[0-9]	1	3	o (m if 3ds_chmobilephone exists)

Name	Description	Type	min	max	m/o/c
3ds_chworkphone	The work phone provided by the Cardholder, without the country code	[0-9]	0	18	o
3ds_workphonecountry	Country Code of the work phone.	[0-9]	1	3	o (m if 3ds_chworkphone exists)
3ds_shipaddrcity	City of the shipping address requested by the Cardholder.	[a-zA-Z]	3	32	o
3ds_shipaddrcountry	Country of the shipping address requested by the Cardholder. Please refer to ISO 3166-1-alpha-2 for a list.	[A-Z]	2	2	c m – if 3ds_shipaddrstate exists or if shipping information is not the same as billing information
3ds_shipaddrline1	First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.	[a-zA-Z]	0	50	o m – when 3ds_addrmatch = false
3ds_shipaddrline2	Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.	[a-zA-Z]	0	50	o m – when 3ds_addrmatch = false
3ds_shipaddrpostcode	ZIP or other postal code of the shipping address associated with the card used for this purchase.	[a-z0-9]	0	16	o m – when 3ds_addrmatch = false
3ds_shipaddrstate	The state or province of the shipping address associated with the card used for this purchase. The value should be the country subdivision code defined in ISO 3166-2.	[0-9]	1	3	o m – when 3ds_addrmatch = false

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

Name	Description	Type	min	max	m/o/c
3ds_deliverytimeframe	Indicates the merchandise delivery timeframe. Accepted values are: 01 - Electronic Delivery 02 - Same day shipping 03 - Overnight shipping 04 - Two-day or more shipping	[0-4]	2	2	o
3ds_deliveryemailaddress	For electronic delivery, the email address to which the merchandise was delivered.	email	7	64	o
3ds_reorderitemsind	Indicates whether the cardholder is reordering previously purchased merchandise. Accepted values are: 01 - First time ordered 02 - Reordered	[0-2]	2	2	o
3ds_preorderpurchseind	Indicates whether the cardholder is placing an order for merchandise with a future availability or release date. Accepted values are: 01 - Merchandise available 02 - Future availability	[0-2]	2	2	o
3ds_preorderdate	For a pre-ordered purchase, the expected date that the merchandise will be available. Date format must be YYYYMMDD.	[0-9]	8	8	o
3ds_giftcardamount	For a prepaid or gift card purchase, the purchase amount total of the prepaid or gift card(s) in major units (for example, USD 123.45 is 123).	[0-9]	1	12	o
3ds_giftcardcurr	For a prepaid or gift card purchase, the currency code of the card as defined in ISO 4217-alpha-3 except for 955 - 964 and 999.	[0-9]	3	3	o

Name	Description	Type	min	max	m/o/c
3ds_giftcardcount	For a prepaid or gift card purchase, the total count of the individual prepaid or gift cards/codes purchased. Field is limited to 2 characters.	[0-9]	0	2	o
3ds_purchasedate	Date and time of the purchase expressed in UTC. The field is limited to 14 characters, formatted as YYYYMMDDHHMMSS.	[0-9]	14	14	m
3ds_recurringexpiry	Date after which no further authorisations shall be performed. This field is limited to 8 characters, and the accepted format is YYYYMMDD. This field is required if a9=1 or 2	[0-9]	8	8	c
3ds_recurringfrequency	Indicates the minimum number of days between authorisations. The field is limited to 4 characters. This field is required if a9=1 or 2	[0-9]	0	4	c
3ds_transtype	Identifies the type of transaction being authenticated. The values are derived from ISO 8583. Accepted values are: 01 - Goods / Service purchase 03 - Check Acceptance 10 - Account Funding 11 - Quasi-Cash Transaction 28 - Prepaid activation and Loan	[0-9]	2	2	m
3ds_merchantname	Assigned merchant name (with a prefix of “http://” or “https://”)	[a-zA-Z0-9]	1	25	o
3ds_browseracceptheader	Exact content of the HTTP accept headers.	[a-zA-Z0-9]	0	2048	o m if 3ds_channel=02
d1	IP address of the browser as returned by the HTTP headers. Supports both ipv4 & ipv6 formats.	ip	7	48	c m if 3ds_channel=02

Name	Description	Type	min	max	m/o/c
					m for Visa 3ds transactions
3ds_browserjavaenabled	Boolean (true/false) that represents the ability of the cardholder browser to execute Java. This field is required for requests where 3ds_channel = 02 (Browser).	[a-z]	4	5	o m if 3ds_channel=02
3ds_browserjavascriptenabled	Boolean that represents the ability of the cardholder browser to execute JavaScript. Accepted values are true / false	[a-z]	4	5	o m if 3ds_channel=02
d6	Value representing the browser language as defined in IETF BCP47. For example: en-GB	[A-Za-z,-]	2	16	o m if 3ds_channel=02
3ds_browsercolordepth	Value representing the bit depth of the colour palette for displaying images, in bits per pixel. Accepted values are: 1 - 1 bit 4 - 4 bits 8 - 8 bits 15 - 15 bits 16 - 16 bits 24 - 24 bits 32 - 32 bits 48 - 48 bits	[0-9]	1	2	o m if 3ds_channel=02
3ds_browserscreenheight	Total height of the Cardholder's screen in pixels.	[0-9]	1	6	c m if 3ds_channel=02, m for Visa 3ds transactions
3ds_browserscreenwidth	Total width of the Cardholder's screen in pixels.	[0-9]	1	6	c, m for Visa 3ds transactions, m if 3ds_channel=02

Name	Description	Type	min	max	m/o/c
3ds_browsertz	Time difference between UTC time and the Cardholder browser local time, in minutes.	[0-9,-]	1	5	o m if 3ds_channel=02
d5	Exact content of the HTTP user-agent header.	[a-zA-Z0-9]	5	255	o m if 3ds_channel=02
3ds_challengewindowsize	Dimensions of the challenge window that will be displayed to the cardholder. The issuer replies with content that is formatted to appropriately render in this window to provide the best possible user experience. Preconfigured window sizes are given in “width x height” in pixels. Accepted values are: 01 - 250 x 400 02 - 390 x 400 03 - 500 x 600 04 - 600 x 400 05 - Full screen	[0-5]	2	2	o m if 3ds_channel=02
3ds_sdkappid	Universally unique ID created upon all installations and updates of the merchant App on a customer device. This is newly generated and stored by the 3DS SDK for each installation or update. The field must have a canonical form as defined in IETF RFC 4122.	[0-9a-zA-Z]	0	36	o m if 3ds_channel=01
3ds_sdkencdata	JWE object, as a string containing data encrypted by the SDK for the DS to decrypt. The field is sent from the SDK. The data will be present when sending to DS, but not present from DS to ACS.	[0-9a-zA-Z]	0	64k	o m if 3ds_channel=01
3ds_sdkephempubkey	Public key component of the ephemeral key pair generated by the 3DS SDK and used to establish	[0-9a-zA-Z]	0	255	o m if 3ds_channel=01

Name	Description	Type	min	max	m/o/c
	session keys between the 3DS SDK and ACS.				
3ds_sdkmaxtimeout	The maximum amount of time (in minutes) for all exchanges. The value must be greater than or equal to 05.	[0-9]	2	2	o m if 3ds_channel=01
3ds_sdkreferencenumber	Identifies the vendor and version of the 3DS SDK that is integrated in a merchant app, assigned by EMVCo when the 3DS SDK is approved.	[0-9a-z]	0	32	o m if 3ds_channel=01
3ds_sdktransid	Universally unique transaction identifier assigned by the 3DS SDK to identify a single transaction. The field must have a canonical form as defined in IETF RFC 4122.	[0-9]	0	36	o m if 3ds_channel=01

Response parameters

Name	Description	Type	min	max	m/o/c
3ds_whiteliststatussource	Is populated by the Whitelist Status system setting. Possible values: 01 = 3DS Server 02 = DS 03 = ACS 04-79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) 80-99 = Reserved for DS use Note: This is a response parameter only	[0-9]	2	2	o
3ds_whiteliststatus	Indicates on the merchant's whitelisting status as confirmed by the ACS. Possible values: true – Merchant is whitelisted by cardholder false – Merchant is not whitelisted by cardholder	[a-z]	4	5	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.

Smart 3D Secure Standalone – Required Fields

In Smart 3D Secure standalone scenarios: For every transaction that participates in the 3D Secure flow, you must send the following fields in addition to the 3D Secure parameters (operation [98]):

Field name	Type	M/O	Description
3ds_merchant_name	String (4,40)	M	Th 3DS merchant name as assigned by the acquirer
3ds_acquirer_bin	Numeric (6,12)	M	The acquirer BIN number
3ds_acquirer_password	String (8,32)	O	The 3D Secure authentication password as assigned by the acquirer
3ds_acquirer_mid	String (4,32)	M	The 3D Secure merchant ID as assigned by the acquirer
3ds_merchant_url	String (4,256)	M	The merchant URL (website)
3ds_merchant_country	Numeric (3,3)	M	The merchant country
3ds_merchant_mcc	Numeric (4,4)	M	The merchant category code (MCC) as assigned by the acquirer

Field name	Type	M/O	Description
3ds_requestorid	Alphanumeric (35 max)	M (relevant only for 3DS v2)	The unique 3D Secure requestor id. Depends on whether you are: • Providing 3DS Standalone to Multiple Merchants • Using 3DS Standalone as a Single Merchant
3ds_requestorname	Alphanumeric (40 max)	M (relevant only for 3DS v2)	The unique 3D Secure requestor name. Depends on whether you are: • Providing 3DS Standalone to Multiple Merchants • Using 3DS Standalone as a Single Merchant

Providing 3DS Standalone to Multiple Merchants

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

- **3DS_requestorname** must be a unique merchant name assigned by the partner
- **3DS_requestorid** 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 during the initial setup Shift4 will provide you with the following details:

- 3DS_requestorname
- 3DS_requestorid

Appendix J: How to Provide 3D Secure Data on the i8 Parameter

This section describes the specifications of the i8 parameter, 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 I: 3D secure.

3D secure data is transmitted via the [i8] parameter.

The [i8] field consists of the following 3 subfields, delimited by a colon:

- ECI (Electronic Commerce Indicator)
- CAVV/AAV
- XID

Note:

- If you have more than one payment processor configured with your Shift4 Gateway account, you must send the r1 parameter as part of the transaction. The value of the parameter should indicate the processor used for 3D Secure authentication. A mismatch between the 3DS processor and the transaction processing processor may result in a decline.
- If you only have one processor, you do not have to provide the r1 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:

Mastercard/Maestro ECI 06 and Visa ECI 07 with the presence of CAVV value, implies that an exemption request was submitted by the acquirer as part of the 3D Secure request, and was approved by the issuer.

CAVV/AAV and XID

Mastercard AAV (UCAF)

Mastercard SecureCode transactions must include an Accountholder Authentication Value (AAV). This means that the AAV tag must be included as part of the 3D Secure [i8] parameter for every Mastercard SecureCode transaction that is transmitted to the *Shift4* Payment API.

Transactions without an AAV will be automatically downgraded to a regular eCommerce transaction and will not benefit from the liability shift and other advantages of an attempted SecureCode transaction.

Encoding - Visa/JCB/American Express/Diners/Discover

The Cardholder Authentication Verification Value (CAVV) and XID should be base-64 decoded (assuming the Merchant Plug-In (MPI) passes back a base-64 encoded value, which is usually the case). After base-64 decoding, the value should be hex-encoded and transmitted in subfield 2 of the [i8] parameter (see Hex-encoding for Visa). If a CAVV value is not available, use "none" as a placeholder.

The XID is mandatory. If an XID value is not available from the MPI, a 40-byte numeric value (ASCII) should be generated and then hex-encoded.

Visa example:

```
i8=05:0700100908808809000013529880881058cb3a65:3030303030303030303030303030303030353030

i8=06:0000010316617700000003030161770000000000:3030303030303030303030303030303030353030

i8=06:none:20202020202020202020313531333833303034
```

Encoding – Mastercard / Maestro

The AAV (UCAF) should be transmitted in subfield 2 of the [i8] parameter with base-64 encoding. This should mean simply passing the value received from the MPI, assuming the MPI passes back a base-64 encoded value. If a CAVV/AAV value is unavailable, use "none" as a placeholder.

Note:

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

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:

```
i8=02:jJ81HADVRtXfCBATEp01CJUAAAA=:00000000000000000501
i8=01:jJ81HADVRtXfCBATEp01CJUAAAA=:00000000000000000501
```

Note:

- Attempted Mastercard and Maestro authenticated transaction may not exceed 10% of the total number of Secure Code transactions
- Shift4 does not participate in the Mastercard/Maestro Advanced Registration and Maestro Recurring Payments programs, and as such doesn not support static AAV. The gateway will thus reject Secure Code transaction where the UCAF transmitted via the i8 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: AAABAxZhdwAAAAMDAWF3AAAAAAA=
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:

- The XID sub-field is not required as part of the i8 parameter. Instead send “none”.
- In addition, send the following parameters as part of the request:

Parameter name	Description	Format	Min,Max
3ds_version	Indicates the 3D Secure protocol version Possible values: 1.0 2.0 2.1.0 2.2.0	[0-9]	3,5
3ds_dstrxid	3DS Directory server transaction ID. Must be sent if 3ds_version = 2.0 or higher and i8 is used.	[0-9A-Za-z,-]	36

Appendix K: Ancillary Fee Codes

Ancillary fee codes are used by travel agencies and airlines. The following table lists the possible ancillary fee codes that can be sent with parameters **an1** - **an4**.

Code	Description
BF	Bundled Service
BG	Baggage Fee
CF	Change Fee
CG	Cargo
CO	Carbon Offset
FF	Frequent Flier
GF	Gift Card
GT	Ground Transport
IE	In-Flight Entertainment
LG	Lounge
MD	Medical
MK	Meal/Beverage
OT	Other
PA	Passenger Assist Fee
PT	Pets
SA	Seat Fee
SB	Standby
SF	Service Fee
ST	Store
TS	Travel Service
UN	Unaccompanied Travel
UP	Upgrades
WI	Wi-Fi

Change History

Version	Subject/Date	Description
1.9 rev 6	May 2024	• Changed the requirement of the following parameters from o to c (m for Visa 3ds transactions): o c1 o c2 o c3 o d1 o 3ds_browserscreenheight o 3ds_browserscreenwidth • Added Response field for AFT transaction 'funding'. • Updated supported currencies: HRK was removed, ZWR was removed, SLL changed to SLE.
1.9 rev 5	March 2024	• Update parameters j5, j6, j7, j8, j9, j13 as mandatory for AFT (Account Funding Transactions) • Update MAC values in parameter z44 • Update a9 values – value names of 01, 02, added 11, 12 • Update available currencies in Appendix H – Transaction Currencies: Remove EEK, LTL, MRO, STD. • Fixe a19 values – 11= Annually
1.9 rev 4	November 2023	• Rebranded to Shift4
1.9 rev 3	April 2023	• Update request parameter 3ds_whiteliststatus validations, add 3ds_whiteliststatus as a response parameter • Add a new value for a10 parameter: 3 = Deffered Authorisation • Allowed to be sent also Sale and Authorisation op codes. • Fixed length of parameter b21, added a possible value in b21, deleted opcode [23] from a4 parameter in Use Token Operations, added note to a9 parameter in Create Token Operation about rejection response from transmitting value 2 for [28], deleted note of a9 parameter in Use Token Operation about rejection response from transmitting value 5 for [23], deleted a13 parameter, updated the max length of 3ds_dstrxid parameter • Fixed request parameter h15 requirements

Version	Subject/Date	Description
1.9 rev 2	January 2022	• Updated CFT void note • added response parameter 3ds_acstrxid • added and updated processing response reason codes: 46, 59, 74, 78, 82, N3, N4 • updated z21 values -97, -98 descriptions • clarified description of 3ds_merchantname • added Discover section to "3DS Standalone to Multiple Merchant" • updated ECI values - 00, 06, 07
1.9 rev 1	November 2021	Updated Visa requirements for sending all merchant-initiated-transactions with a proper 'initial transaction id' (and not a generic value) using the g6 parameter.
1.9	November 2021	New functionality: Incremental Authorisation: • New operation code [20] • Updated functionality of request parameters a4 and a9 when used with incremental authorisation • New response parameter z25 – updated amount
1.8 rev 12	September 2021	Edited the description of the SmartGuard service
1.8 rev 11	September 2021	Added a possible value in b21 Changed the ISK currency exponent Added parameter z44, response code 79 and result value 07 Edited the description of special operations 34. 35
1.8 rev 10	July 2021	Added clarification regarding the a10 parameter
1.8 rev 9	July 2021	Added response parameters z35, z36, z37 Changed max length of c1
1.8 rev 8	June 2021	Changed token_cavv parameter name to be token_crypto

Version	Subject/Date	Description
1.8 rev 7	June 2021	Changed optional/mandatory requirements for j6, j7, j8, j9 parameters in CFT transactions. Changed j8 minimum length. Fixed the format of b20, Added N7 to Processing Response Reason Codes Addition of additional value of “Cartes Bancaires “ for b2 Changed max length of c1, minimum length of 3ds_shipaddrstate, j11 format, max length of 3ds_acquirer_bin Change single and double quotation marks in Message Cipher Added values to smart_3ds_result Addition of optional reason for to z2=-38 description (z3)
1.8 rev 6	May 2021	Added Seller Information parameter h15 Changed optional/mandatory requirements for c1, c3 parameters in CFT transactions
1.8 rev 5	May 2021	Added Credorax stand-in service parameter z43
1.8 rev 4	April 2021	Changed optional/mandatory requirements for c4, c5, c7, c8, c9, j5, j13 parameters in CFT transactions
1.8 rev 3	March 2021	Updated ota3 description, content of fl1, fl2, fl3, fl4 Removed 3ds fields which are not in use
1.8 rev 2	February 2021	Changed fl5 and fl6 min and max length Changed value of exemption_reason in tra_score description Changed explanation of 3ds_recurringexpiry and 3ds_recurringfrequency Changed type of d6 and added an example
1.8 rev 1	January 2021	Changed the length of the 3ds_version parameter Added g6 to the Use Token Operations table Added recommendation for 3DS v1.0 cardholder challenge flow
1.8	December 2020	Addition of 3DS v2.2-related Decoupled Authentication, Whitelisting and Authentication fields and settings as well as several other small changes and additions.
1.7 rev 1	November 2020	Addition of Smart 3D Secure standalone services
1.7	October 2020	Added information how to send transactions that were originally processed by Apple Pay or Google Pay wallets Removed the following currencies: CUP, IRR, KPW, SDG Added clarification when to send g6

Version	Subject/Date	Description
1.6 rev 2	September 2020	Added new opcodes [88] and [89] allowing to create a token and use a token for 3D Secure authentication-only flow
1.6 rev 1	August 2020	Changed Optional/Mandatory requirements of Funds Recipient parameters
1.6	August 2020	Added parameter a1 to opcode [92] mandatory parameters table Added new parameter a14: partial authorisation tag
1.5 rev 2	August 2020	Added new response parameter b20 - Payment Account Reference (PAR)
1.5 rev 1	July 2020	Introduced partial authorisation void Changed Optional/Mandatory requirements of Funds Recipient parameters Added MCCs relevant for the Referral CFT operation Modified 3D Secure workflow diagrams Added new parameter a13 Added new Request parameters: Amount Components, Furniture, Car, Plane and Boat Rentals, Event Management, some Travel parameters
1.5	May 2020	Removed the 3ds_smartplan parameter Addition of new processing response reason codes
1.4 rev 4	April 2020	Operation codes clarifications
1.4 rev 3	April 2020	Minor bug fixes
1.4 rev 2	March 2020	Addition of new operation result codes
1.4 rev 1	March 2020	Addition of new Ancillary Fee Codes appendix
1.4	February 2020	Addition of new travel parameters Addition of new parameter h8 Addition of new response parameter z55
1.3	November 2019	Addition of op codes 104,105 & z51 Addition of "04" value for 3ds_initiate, and decommission of 3ds_smarttype parameter Changed 3ds_transtype from being Optional to being Mandatory Minor text & formatting corrections
1.2 rev 4	October 2019	Minor format corrections
1.2 rev 3	September 2019	Minor format corrections Changed the values of Low value exemption & Low Risk Exemption
1.2 rev 2	July 2019	Clarification on the Hashing algorithm logic Additional Value “C” for the 3ds_status field Added required parameter “g1” for op code [38]

Version	Subject/Date	Description
1.2	July 2019	Addition of exemption management section Addition of two new response values in z6 parameter (70, 1A) Addition of three new response codes in z2 parameter (-64, -65, -66) Addition of new g6 referral operation parameter Addition of new z50 response-field parameter
1.1	May 2019	Addition of 3DS Adviser fields – exemption management Clarification regarding using 3D Secure with a third party provider
1.0 rev 4	March 2019	Changes to mandatory parameters due to 3D secure
1.0 rev 3	March 2019	Clarification of z13 parameter description
1.0 rev 2	March 2019	Clarification about required/optional parameters Clarification about how to send the i8 for 3D secure version 2.0 Two new response codes related to the 3D secure flow (-37, -13)
1.0 rev 1	March 2019	Guidelines for 3D Secure 2.0 for using third party 3D Secure providers
1.0	February 2019	First release

Need Support?

Contact our 24/7 Client Relations Centre 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