Source Payment Gateway

API Specification

API Version 1.9 rev 2

January 2022
## Contents

- **Introduction** .................................................................................................................. 6
  - Glossary .............................................................................................................................. 6
  - Useful Documents / References .......................................................................................... 7
  - Certification .......................................................................................................................... 8
  - API Version Control ............................................................................................................ 8
  - Publisher Information ......................................................................................................... 8
- **Gateway Interface** .............................................................................................................. 9
  - Introduction ......................................................................................................................... 9
  - Uniform Resource Locators (URLs) ..................................................................................... 9
  - HTTP Specification ............................................................................................................. 9
    - Example HTTP Request .................................................................................................... 10
  - Security/Authentication ....................................................................................................... 10
  - Health Checks ....................................................................................................................... 10
- **Gateway Features** ............................................................................................................. 12
  - Address Verification System (AVS) .................................................................................... 12
  - Card-Present ....................................................................................................................... 12
  - Card Validation .................................................................................................................... 12
  - CVV/CVV2/CVC2 .................................................................................................................. 12
  - Dynamic Descriptor ............................................................................................................ 13
  - SmartGuard ........................................................................................................................ 13
  - Smart Routing ..................................................................................................................... 13
  - Token Engine (Card-on-File) ............................................................................................. 14
  - 3D Secure ........................................................................................................................... 14
- **Required Fields** ................................................................................................................ 15
  - Basic Operations .................................................................................................................. 15
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referral Operations</td>
<td>22</td>
</tr>
<tr>
<td>Token (Card-on-file) Operations</td>
<td>29</td>
</tr>
<tr>
<td>Create Token Operations</td>
<td>30</td>
</tr>
<tr>
<td>Use Token Operations</td>
<td>39</td>
</tr>
<tr>
<td>Referral Token Operations</td>
<td>46</td>
</tr>
<tr>
<td>Special Operations</td>
<td>51</td>
</tr>
<tr>
<td>Data Retrieval Operations</td>
<td>55</td>
</tr>
<tr>
<td>Response Fields</td>
<td>59</td>
</tr>
<tr>
<td>Appendix A: Message Cipher</td>
<td>67</td>
</tr>
<tr>
<td>Appendix B: Operation Result Codes</td>
<td>69</td>
</tr>
<tr>
<td>Appendix C: AVS Response Codes</td>
<td>71</td>
</tr>
<tr>
<td>Appendix D: Processing Response Reason Codes</td>
<td>73</td>
</tr>
<tr>
<td>Appendix E: z21 Possible Values</td>
<td>76</td>
</tr>
<tr>
<td>Appendix F: Additional Request Parameters</td>
<td>77</td>
</tr>
<tr>
<td>User Device Information</td>
<td>77</td>
</tr>
<tr>
<td>Retail</td>
<td>77</td>
</tr>
<tr>
<td>Gaming</td>
<td>77</td>
</tr>
<tr>
<td>Forex</td>
<td>78</td>
</tr>
<tr>
<td>Streaming</td>
<td>78</td>
</tr>
<tr>
<td>Amount Components</td>
<td>78</td>
</tr>
<tr>
<td>Furniture</td>
<td>78</td>
</tr>
<tr>
<td>Car, Plane and Boat Rentals</td>
<td>79</td>
</tr>
<tr>
<td>Event Management</td>
<td>79</td>
</tr>
<tr>
<td>Travel</td>
<td>79</td>
</tr>
<tr>
<td>Customer Identity</td>
<td>82</td>
</tr>
<tr>
<td>Appendix G: r1 Possible Values</td>
<td>83</td>
</tr>
<tr>
<td>Appendix H: Transaction Currencies</td>
<td>84</td>
</tr>
</tbody>
</table>
Appendix I: SCA & 3D Secure ................................................................. 90
3D Secure and Customer Experience: Frictionless Experience vs. Cardholder Challenge ............. 90
3D Secure Transaction Flow ........................................................................ 91
   Initiating the 3D Secure process ............................................................... 91
   Standard 3D Secure Workflow ................................................................. 92
      Flow A: No challenge (frictionless experience) flow .................................. 93
      Flow B: 3D secure process requires device fingerprint assessment .................. 94
      Flow C: 3D secure requires a user challenge flow (redirection to issuer) ............... 95
      Flow D: 3D secure flow requires fingerprint authentication and user challenge .......... 96
   Device fingerprint information retrieval flow ............................................ 97
   Cardholder challenge flow ....................................................................... 98
   3DS Adviser ....................................................................................... 99
Strong Customer Authentication (SCA) ................................................................ 100
   Exemption management .......................................................................... 100
   Managing SCA for Merchant initiated transaction ...................................... 102
   Exemption – Response Parameters .......................................................... 102
   3D Secure Authentication-Only Flow ....................................................... 102
   Additional Parameters for Improved 3D Secure Assessment ....................... 103
      Recommended Parameters ..................................................................... 103
      Request parameters ............................................................................ 104
      Response parameters .......................................................................... 120
Smart 3D Secure Standalone Services .................................................................. 120
   Initial Setup .......................................................................................... 120
   Smart 3D Secure Standalone – Required Fields ......................................... 121
   Providing 3DS Standalone to Multiple Merchants ....................................... 122
   Using 3DS Standalone as a Single Merchant ............................................ 122
Appendix J: How to Provide 3D Secure Data on the i8 Parameter ......................... 123
**Introduction**

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

The Source 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 Source 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 Source 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**

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Gateway</td>
<td>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.</td>
</tr>
<tr>
<td>Payment Processor</td>
<td>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.</td>
</tr>
<tr>
<td>Authorisation</td>
<td>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.</td>
</tr>
<tr>
<td>Capture</td>
<td>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.</td>
</tr>
<tr>
<td>Sale</td>
<td>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.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Void</td>
<td>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.</td>
</tr>
<tr>
<td>Credit</td>
<td>There are two types of Credit requests: (1) <strong>Referral Credit</strong>, a request that instructs the Gateway to refund a previously captured transaction to the cardholder, and (2) <strong>Independent Credit</strong>, a request that initiates a stand-alone credit transaction. Full card number is needed.</td>
</tr>
<tr>
<td>CFT</td>
<td>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).</td>
</tr>
<tr>
<td>AVS</td>
<td>The Address Verification System (AVS) is a security measure for verifying the address of a person claiming to own a credit card.</td>
</tr>
<tr>
<td>Token Transactions</td>
<td>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.</td>
</tr>
<tr>
<td>ZIP+4</td>
<td>An expanded ZIP code system used by the U.S. Postal Service that uses the basic five-digit code plus four additional digits.</td>
</tr>
</tbody>
</table>
| 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 **Source** 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 Source Payment Gateway API Specification:  
  - [Source Card-Present Specification](#) – a supplement to the **Source Gateway API Specification** that provides detailed information on the API’s use of Card-Present data.
• *Source Processors documentation* - select the specification for the processor you work with, can be found on the [Credorax 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@credorax.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**

Copyright © Source Ltd. All rights reserved.
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 Source 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=4545454545454545&b2=1&b3=08&b4=11&b5=003&c1=John+Smith&c3=johnsmith@yahoo.com&d1=111.222.0.101

Note:
- Please honour a TTL of at least 30 seconds for each single session per HTTPS request.
- Each processor may have a different TTL. Please refer to the Credorax Worldwide Processors specification documents for further information.

Security/Authentication

All HTTP requests must be sent through a secure channel and over SSL (Secure Sockets Layer). The Source 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 Source Payment Gateway and Integration Environments by accessing the following URLs:

<table>
<thead>
<tr>
<th>Testing</th>
<th>Integration Environment</th>
<th><a href="https://intconsole.credorax.com/intenv/service/status">https://intconsole.credorax.com/intenv/service/status</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Production</td>
<td>Production Environment</td>
<td><a href="https://xts.gate.credorax.net/brain/rest/health">https://xts.gate.credorax.net/brain/rest/health</a></td>
</tr>
</tbody>
</table>
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 Credorax Client Relations Team immediately in the event of any unexpected service interruption, at:

support@credorax.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 Source 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 Source) 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 Credorax 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 Smart Guard service requires prior registration. Contact your 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 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.

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

The Source 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 on the Source Payment Gateway products and services, contact your account manager.
Required Fields

The Source Payment Gateway provides 4 operation groups:

1. Basic operations
2. Referral operations
3. Token operations (Card-on-File)
4. 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. Please refer to the Source Payment Gateway: Processors Specification document for further information.

Basic Operations

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

<table>
<thead>
<tr>
<th>Basic Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1] Sale</td>
</tr>
<tr>
<td>[2] Authorisation</td>
</tr>
<tr>
<td>[6] Independent Credit</td>
</tr>
</tbody>
</table>

[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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length (min,max)</th>
<th>Stand-Alone Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Source assigned gateway merchant ID</td>
<td>[A-Z0-9_]</td>
<td>3,8</td>
<td>m</td>
</tr>
<tr>
<td>K</td>
<td>Unique cipher used for authenticating requests</td>
<td>[0-9A-Za-z]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code</td>
<td>[0-9]</td>
<td>1,3</td>
<td>m</td>
</tr>
<tr>
<td>a1</td>
<td>Request ID</td>
<td>[A-Za-z0-9-]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td>a2</td>
<td>Payment source type</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o</td>
</tr>
<tr>
<td>a4</td>
<td>Requested billing amount</td>
<td>[0-9]</td>
<td>1,12</td>
<td>m</td>
</tr>
<tr>
<td>a5</td>
<td>Transaction currency</td>
<td>[A-Z]</td>
<td>3,3</td>
<td>m</td>
</tr>
<tr>
<td>a6</td>
<td>Transaction date (local date of the transaction)</td>
<td>yyyyMMdd</td>
<td>6,6</td>
<td>o</td>
</tr>
<tr>
<td>a7</td>
<td>Transaction time (local time of the transaction)</td>
<td>HHmmss</td>
<td>6,6</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min,max)</td>
<td>Stand-Alone Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>a9</td>
<td>Transaction type. Valid values are:</td>
<td>[0-9]</td>
<td>1,2</td>
<td>c ([1], [2] for recurring)</td>
</tr>
<tr>
<td></td>
<td><strong>Value</strong></td>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>First recurring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Subsequent recurring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>Card-Only Validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>Straight Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>Unscheduled Card-on-File transactions initiated by the merchant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>Unscheduled Card-on-File transactions initiated by the cardholder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>Card validations for an unscheduled Card-on-File</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
By default, the transaction type is considered a straight operation unless specified otherwise.

<table>
<thead>
<tr>
<th>a10</th>
<th>Authorisation Type:</th>
<th>[1-2]</th>
<th>1,1</th>
<th>o ([2] only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Final Authorisation (default value)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Pre-Authorisation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transactions referring to Pre-Authorisations must include an a4 parameter.

<table>
<thead>
<tr>
<th>a11</th>
<th>Multiple Capture tag</th>
<th>[0-9]</th>
<th>1,2</th>
<th>o ([2] only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Indicates the number of expected Captures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only supported in Card-not-Present transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value is 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Max value is 98</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Min value is 2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>a14</th>
<th>Partial Authorisation tag</th>
<th>[0,1]</th>
<th>1,1</th>
<th>o ([2] only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This request parameter indicates to the issuer whether you are willing to accept partial authorisation approval. Possible values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 – Full authorisation only (default)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 – Partial authorisation also accepted</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>b1</th>
<th>PAN – Primary Account Number</th>
<th>[0-9]</th>
<th>8,19</th>
<th>m</th>
</tr>
</thead>
<tbody>
<tr>
<td>b3</td>
<td>Card expiration month</td>
<td>[0-9]</td>
<td>2,2</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Two-digit number (mm format)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b4</td>
<td>Card expiration year</td>
<td>[0-9]</td>
<td>2,2</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Two-digit number (yy format)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min,max)</td>
<td>Stand-Alone Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>b5</td>
<td>Card security code (CVV / CVC) as printed on the card</td>
<td>[0-9]</td>
<td>3,4</td>
<td>m (o for [6])</td>
</tr>
<tr>
<td>b21</td>
<td>Passthrough wallet indicator</td>
<td>[A-Za-z\ ]</td>
<td>9-12</td>
<td>c (m if transaction was originally Apple Pay, Google Pay or VTS/M4M transaction)</td>
</tr>
<tr>
<td>c1</td>
<td>Cardholder's full name</td>
<td>[\ a-zA-Z]</td>
<td>5,45</td>
<td>c recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>c2</td>
<td>Cardholder's contact phone number</td>
<td>[0-9-.]</td>
<td>5,32</td>
<td>o</td>
</tr>
<tr>
<td>c3</td>
<td>Cardholder's email address</td>
<td>email</td>
<td>7,64</td>
<td>o</td>
</tr>
<tr>
<td>c4</td>
<td>Cardholder Billing Address street number</td>
<td>[0-9]</td>
<td>1,16</td>
<td>o recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>c5</td>
<td>Cardholder Billing Address street name</td>
<td>[a-zA-Z0-9\ -\ ]</td>
<td>4,50</td>
<td>o recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>c7</td>
<td>Cardholder Billing Address city name</td>
<td>[a-zA-Z\ -\ ]</td>
<td>3,30</td>
<td>o recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>c8</td>
<td>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.</td>
<td>[a-zA-Z0-9-]</td>
<td>1,3</td>
<td>o recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min,max)</td>
<td>Stand-Alone Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>-----------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>c10</td>
<td>Cardholder Billing Address Postal/ZIP Code</td>
<td>[a-zA-Z0-9-\ ]</td>
<td>1,9</td>
<td>c recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>d1</td>
<td>Cardholder IP Address</td>
<td>[0-9-.]</td>
<td>7,15</td>
<td>m</td>
</tr>
<tr>
<td>d2</td>
<td>Echo parameter</td>
<td>[a-zA-Z0-9]</td>
<td>3,128</td>
<td>o</td>
</tr>
<tr>
<td>f21</td>
<td>Boolean field specifying whether the fraud protection service check should be bypassed.</td>
<td>[0-1]</td>
<td>1,1</td>
<td>o(n/a for [6])</td>
</tr>
<tr>
<td></td>
<td><strong>Value</strong></td>
<td><strong>Description</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Send for a fraud check. (default value)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Do not send for a fraud check</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only available to merchants using the Smart Guard fraud protection service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f22</td>
<td>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.</td>
<td>[0-9]</td>
<td>0,4</td>
<td>o(n/a for [6])</td>
</tr>
<tr>
<td>h3</td>
<td>Sub-Merchant ID</td>
<td>[0-9]</td>
<td>1,15</td>
<td>c (Payment Facilitators)</td>
</tr>
<tr>
<td>h8</td>
<td>Sub-Merchant’s telephone number</td>
<td>[0-9-.]</td>
<td>5,32</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min,max)</td>
<td>Stand-Alone Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h15</td>
<td>Seller Information</td>
<td>[a-zA-Z0-9-|-]</td>
<td>9,164</td>
<td>o ([1], [2] only)</td>
</tr>
<tr>
<td></td>
<td>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 &quot;|&quot;. <strong>Note:</strong> This field is used by marketplaces.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Length (min, max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller ID</td>
<td>[a-zA-Z0-9-|-]</td>
<td>4,64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller country</td>
<td>[A-Z]</td>
<td>3,3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller city</td>
<td>[a-zA-Z-|-]</td>
<td>3,30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller street</td>
<td>[a-zA-Z0-9-|-]</td>
<td>4,50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller zip code</td>
<td>[a-zA-Z0-9-|-]</td>
<td>1,9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller state</td>
<td>[a-zA-Z0-9]</td>
<td>3,3</td>
<td></td>
<td></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</td>
<td>Text</td>
<td>1,39</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min,max)</td>
<td>Stand-Alone Operations</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>i8</td>
<td>3D Secure Data</td>
<td>[a-zA-Z0-9:=+]</td>
<td>10,128</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Composed of 3 different parameters delimited by a colon:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. ECI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. CAVV/AAV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. XID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="#">Appendix J: How to Provide 3D Secure Data on the i8 Parameter</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="#">Source Payment Gateway: Processors Specification</a> to learn whether the 3D secure service is supported and which Payment Processors support the transfer of 3DS information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A transmitted i8 will not be routed to Payment Processors that do not support this feature. Furthermore, the transaction will be rejected by the Source 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)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_version</td>
<td>Indicates the 3D Secure protocol version</td>
<td>[0-9]</td>
<td>3.5</td>
<td>c (m if using i8)</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.1.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.2.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_dstrxid</td>
<td>3DS Directory server transaction ID. Must be sent if 3ds_version = 2.0 or higher and i8 is used.</td>
<td>[0-9A-Za-z,-]</td>
<td>34</td>
<td>c (m if 3ds_version = 2.0 or higher)</td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="#">Appendix J: How to Provide 3D Secure Data on the i8 Parameter</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>j1</td>
<td>Primary Account Recipient’s date of birth</td>
<td>YYYYMMDD</td>
<td></td>
<td>c (6012 UK merchant)</td>
</tr>
<tr>
<td>j2</td>
<td>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.</td>
<td>[a-zA-Z0-9-]</td>
<td>8,8</td>
<td>c (6012 UK merchant)</td>
</tr>
<tr>
<td>j3</td>
<td>Primary Account Recipient’s Postal Code</td>
<td>[a-zA-Z0-9 /-]</td>
<td>2,6</td>
<td>c (6012 UK merchant)</td>
</tr>
<tr>
<td>j4</td>
<td>Primary Account Recipient’s partial surname</td>
<td>[a-zA-Z-]</td>
<td>2,6</td>
<td>c (6012 UK merchant)</td>
</tr>
<tr>
<td>j5</td>
<td>Funds Recipient’s First name</td>
<td>[-&quot;A-Za-z]</td>
<td>1,30</td>
<td>o</td>
</tr>
<tr>
<td>j6</td>
<td>Funds Recipient’s Street Address</td>
<td>[&quot;0-9A-Za-z]</td>
<td>1,30</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min,max)</td>
<td>Stand-Alone Operations</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------</td>
<td>-------------------</td>
<td>------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>j7</td>
<td>Funds Recipient's City</td>
<td>[&quot;0-9A-Za-z&quot;]</td>
<td>1,25</td>
<td>o</td>
</tr>
<tr>
<td>j8</td>
<td>Funds Recipient's State/Province Code</td>
<td>[0-9A-Za-z]</td>
<td>2,3</td>
<td>o</td>
</tr>
<tr>
<td>j9</td>
<td>Funds Recipient's Country Code</td>
<td>[A-Z]</td>
<td>3,3</td>
<td>o</td>
</tr>
<tr>
<td>j10</td>
<td>Funds Recipient's Phone Number</td>
<td>[0-9-]</td>
<td>1,20</td>
<td>o</td>
</tr>
<tr>
<td>j11</td>
<td>Funds Recipient's Date of Birth</td>
<td>MMDDYYYY</td>
<td>8,8</td>
<td>o</td>
</tr>
<tr>
<td>j12</td>
<td>Funds Recipient Postal Code</td>
<td>[a-zA-Z0-9 /-]</td>
<td>1,10</td>
<td>o</td>
</tr>
<tr>
<td>j13</td>
<td>Funds Recipient Surname</td>
<td>[A-Za-z]</td>
<td>1,30</td>
<td>o</td>
</tr>
<tr>
<td>r1</td>
<td>Indicates the selected Processor for the specific transaction.</td>
<td>[a-zA-Z0-9]</td>
<td>0,9</td>
<td>o(n/a for [6])</td>
</tr>
<tr>
<td></td>
<td>The transaction is routed according to the transmitted value.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>r2</td>
<td>Indicates the Processor target MID for the specific transaction.</td>
<td>[a-zA-Z0-9]</td>
<td>0,32</td>
<td>o(n/a for [6])</td>
</tr>
<tr>
<td>r3</td>
<td>The routing sequence number.</td>
<td>[1-9]</td>
<td>1,2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_initiate</td>
<td>Indicates whether to initiate the Source 3D Secure</td>
<td>[0-3]</td>
<td>2,2</td>
<td>o (default value: 02)</td>
</tr>
<tr>
<td></td>
<td>Authentication process. Possible values are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01: Initiate 3D Secure before completing the payment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02: Process payment without initiating 3D Secure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03: Initiate 3D Secure according to the 3DS Adviser result</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04: Only initiate the 3DS Adviser service. Relevant only for op</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>code 98.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For additional information about the 3D Secure process, see</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Appendix I: 3D Secure.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If the transaction contains both the 3ds_initiate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>parameter and the i8 parameter, the transaction will</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>be declined.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>token_eci</td>
<td>ECI value returned from the token decryption process</td>
<td>[0-9]</td>
<td>2,2</td>
<td>c (m if transaction is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>scheme token based and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b21 is sent)</td>
</tr>
<tr>
<td>token_crypto</td>
<td>CAVV/AAV value returned from the token decryption process</td>
<td>[A-Za-z0-9]</td>
<td>40,40</td>
<td>c (m if transaction is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>scheme token based and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b21 is sent)</td>
</tr>
</tbody>
</table>

### Referral Operations

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

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[3]</td>
<td>Capture</td>
</tr>
<tr>
<td>[5]</td>
<td>Referral Credit</td>
</tr>
<tr>
<td>[7]</td>
<td>Sale Void</td>
</tr>
<tr>
<td>[8]</td>
<td>Refund Void</td>
</tr>
<tr>
<td>[9]</td>
<td>Capture Void</td>
</tr>
<tr>
<td>[20]</td>
<td>Incremental Authorisation</td>
</tr>
</tbody>
</table>

[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
**Incremental Authorisation**

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

**Required Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Referral Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Source assigned gateway merchant ID</td>
<td>[A-Z0-9_]</td>
<td>3,6</td>
<td>m</td>
</tr>
<tr>
<td>K</td>
<td>Unique cipher used for authenticating requests</td>
<td>[0-9A-Za-z]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="#">Appendix A: Message Cipher</a> for further details on generating the cipher.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O</td>
<td>Operation Code</td>
<td>[0-9]</td>
<td>1,3</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>The operation code is used for determining the requested service. See <a href="#">List of Referral Operations</a>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a1</td>
<td>Request ID</td>
<td>[A-Za-z0-9-]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a2</td>
<td>Payment Source Type</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Valid options are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 Online Order (default value)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 Telephone Order</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Mail Order</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 Virtual Terminal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Referral Operations</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------</td>
<td>--------</td>
<td>---------------------</td>
</tr>
<tr>
<td>a4</td>
<td>Requested billing amount</td>
<td>[0-9]</td>
<td>1,12 m</td>
<td>[3] [4] [5] [7]</td>
</tr>
<tr>
<td></td>
<td>The amount value should not include a decimal point. Amounts in currencies</td>
<td></td>
<td></td>
<td>[8] [9] [20]</td>
</tr>
<tr>
<td></td>
<td>that have two, three or no exponents should be formatted according to their</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>currency requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix H: Transaction Currencies for more information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The amount can be transmitted as part of a referral transaction in order to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>indicate a partial amount (in case of a partial void, a partial refund or a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>partial capture) or to indicate an additional amount (in case of incremental</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>authorisation). In all other cases, a referral transaction defaults to the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>full amount transmitted in the original transaction’s a4 parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a5</td>
<td>Transaction Currency</td>
<td>[A-Z]</td>
<td>3,3 m</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indicates the currency that should be used in the transaction (every currency</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>used must be preconfigured on the Source platform).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to ISO 4217-alpha-3 for further details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a6</td>
<td>Transaction date (current local date of the transaction)</td>
<td>yyMMdd</td>
<td>6,6 o</td>
<td></td>
</tr>
<tr>
<td>a7</td>
<td>Transaction time (current local time of the transaction)</td>
<td>HHmmss</td>
<td>6,6 o</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Referral Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>---------------------</td>
</tr>
<tr>
<td>a9</td>
<td>Transaction type. Valid values are:</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o for [3]</td>
</tr>
<tr>
<td>a13</td>
<td>Final capture indication. In multiple-capture scenarios, use this parameter to indicate whether this capture is the final capture. Valid values are:</td>
<td>[0-9]</td>
<td>1,1</td>
<td>o for [5]</td>
</tr>
<tr>
<td>b3</td>
<td>Card expiration month</td>
<td>[0-9]</td>
<td>2,2</td>
<td>c for [5]</td>
</tr>
<tr>
<td>b4</td>
<td>Card expiration year</td>
<td>[0-9]</td>
<td>2,2</td>
<td>c for [5]</td>
</tr>
<tr>
<td>d1</td>
<td>Cardholder IP Address</td>
<td>[0-9.]</td>
<td>7,15</td>
<td>o</td>
</tr>
</tbody>
</table>

**Value Description**

- **Value**
  - **1**: First recurring
  - **2**: Subsequent recurring
  - **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

By default, the transaction type is considered a straight operation unless specified otherwise.

- **Value**
  - **1**: Final capture
  - **0**: Not final capture

- **Card expiration month**
  - Two-digit number (mm format)

- **Card expiration year**
  - Two-digit number (yy format)

- **Cardholder IP Address**
  - The IP address of the server that is connecting to the Source gateway should always be sent for Card-Present transactions.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Referral Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>d2</td>
<td>Echo parameter</td>
<td>Text</td>
<td>3,128</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Any value up to 128 bytes long transmitted within a request will be</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>returned within the response to this parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: No plaintext cardholder data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>should be provided in this field.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g2</td>
<td>Response ID</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>The z1 parameter from a corresponding past transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g3</td>
<td>Authorisation Code</td>
<td>[a-zA-Z0-9]</td>
<td>1,10</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>The z4 parameter from a corresponding past transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g4</td>
<td>Request ID</td>
<td>[0-9A-Za-z]</td>
<td>1,32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>The a1 parameter from a corresponding past transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g6</td>
<td>Initial transaction ID</td>
<td>[0-9A-Za-z]</td>
<td>13,15</td>
<td>o (m if a9=2 or 8)</td>
</tr>
<tr>
<td></td>
<td>The z50 parameter that was received</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>in the original transaction response.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Must be sent to ensure the transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is considered an MIT transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the transaction is an MIT and the original transaction was prior to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 Sept. 2019, send the following value: 999999999999999.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: As of 1 April 2022 Visa requires that each subsequent transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>includes a proper ‘initial transaction id’ on the g6 parameter. The</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>generic value above will no longer be accepted. This applies to all</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transactions including those initiated before September 2019. If you do not</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>have this value, work with your customers to get a new original transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>authorised and authenticated.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Referral Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>---------------------</td>
</tr>
<tr>
<td>h9</td>
<td>Merchant reference number</td>
<td>Text</td>
<td>1,32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h15</td>
<td>Seller Information</td>
<td>[a-zA-Z0-9-_]</td>
<td>9,164</td>
<td>o ([3] only)</td>
</tr>
<tr>
<td></td>
<td>This field contains seller information. When using this field, &quot;Seller ID&quot; 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 &quot;.&quot;. <strong>Note</strong>: This field is used by marketplaces.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Length (min, max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller ID</td>
<td>[a-zA-Z0-9-_]</td>
<td>4,64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller country</td>
<td>[A-Z]</td>
<td>3,3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller city</td>
<td>[a-zA-Z-_]</td>
<td>3,30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller street</td>
<td>[a-zA-Z0-9-_]</td>
<td>4,50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller zip code</td>
<td>[a-zA-Z0-9-_]</td>
<td>1,9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller state</td>
<td>[a-zA-Z0-9-_]</td>
<td>3,3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i2</td>
<td>Billing Descriptor</td>
<td>Text</td>
<td>1,39</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>The Descriptor that appears on the cardholder's statement. Refer to <em>Source Payment Gateway: Processors Specification</em> to learn whether the Dynamic Descriptor feature is supported. The i2 parameter will be ignored if the processor does not support Dynamic Descriptors.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Token (Card-on-file) Operations

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

<table>
<thead>
<tr>
<th></th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Create Token</td>
</tr>
<tr>
<td>23</td>
<td>Create Token with Sale</td>
</tr>
<tr>
<td>28</td>
<td>Create Token - Auth</td>
</tr>
<tr>
<td>29</td>
<td>Create Token – Capture</td>
</tr>
<tr>
<td>11</td>
<td>Use Token – Sale</td>
</tr>
<tr>
<td>12</td>
<td>Use Token – Auth</td>
</tr>
<tr>
<td>13</td>
<td>Use Token – Capture</td>
</tr>
<tr>
<td>24</td>
<td>Use Token – Recurring Sale</td>
</tr>
<tr>
<td>32</td>
<td>Use Token - Recurring Auth</td>
</tr>
<tr>
<td>33</td>
<td>Use Token – Recurring Capture</td>
</tr>
<tr>
<td>14</td>
<td>Token Auth Void</td>
</tr>
<tr>
<td>15</td>
<td>Token Referral Credit</td>
</tr>
<tr>
<td>16</td>
<td>Block Token</td>
</tr>
</tbody>
</table>
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 preforms card validation using the minimal transaction amount allowed by the selected Payment Processor regardless of the amount transmitted in the request.
- A successful request returns a value of ‘0’ in the z2 parameter 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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Create Token Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Source assigned Gateway Merchant ID</td>
<td>[A-Z0-9_]</td>
<td>3.6</td>
<td>[10]</td>
</tr>
<tr>
<td>K</td>
<td>Unique cipher used for authenticating requests. Refer to Appendix A: Message Cipher for further details on generating the cipher.</td>
<td>[0-9A-Za-z]</td>
<td>1.32</td>
<td>[23] [28]</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code The operation code is used for determining the requested service. See the list in Create Token Operations.</td>
<td>[0-9]</td>
<td>1.3</td>
<td></td>
</tr>
<tr>
<td>a1</td>
<td>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.</td>
<td>[A-Za-z0-9-]</td>
<td>1.32</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>a2</td>
<td>Payment source Type</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Valid options are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 Online Order (default value)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 Telephone Order</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Mail Order</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 Virtual Terminal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a4</td>
<td>Requested Billing Amount</td>
<td>[0-9]</td>
<td>1,12</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix H: Transaction Currencies for more details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The minimum transaction value should be 0.01 EUR (or the equivalent or EUR 0.01 in another currency), otherwise the request is rejected.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a5</td>
<td>Transaction Currency</td>
<td>[A-Z]</td>
<td>3,3</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Indicates the currency that should be used in the transaction (every currency used must be preconfigured on the Source platform).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to ISO 4217-alpha-3 for further information.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a6</td>
<td>Transaction date (local date of the transaction)</td>
<td>yyMMMdd</td>
<td>6,6</td>
<td>o</td>
</tr>
<tr>
<td>a7</td>
<td>Transaction time (local time of the transaction)</td>
<td>HHmmss</td>
<td>6,6</td>
<td>o</td>
</tr>
<tr>
<td>a8</td>
<td>Merchant Invoice ID</td>
<td>text</td>
<td>1,16</td>
<td>c (required for [23], [28])</td>
</tr>
<tr>
<td></td>
<td>Only required for subscription transactions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>a9</td>
<td>Transaction Type. Valid values are:</td>
<td>[0-9]</td>
<td>1,2</td>
<td>[10] [23] [28]</td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>First recurring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Subsequent recurring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Card-Only Validation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Straight Operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Unscheduled Card-on-File transactions initiated by the merchant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Unscheduled Card-on-File transactions initiated by the cardholder</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Card validations for an unscheduled Card-on-File</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>a10</th>
<th>Authorisation Type:</th>
<th>[1-2]</th>
<th>1,1</th>
<th>o ([28] only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Final Authorisation (default value)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Pre-Authorisation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transactions referring to Pre-Authorisations must include an a4 parameter.

<table>
<thead>
<tr>
<th>a11</th>
<th>Multiple Capture tag</th>
<th>[0-9]</th>
<th>1,2</th>
<th>o ([28] only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Indicates the number of expected Captures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only supported in Card-not-Present transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default value is 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Max value is 98</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Min value is 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>a14</td>
<td>Partial Authorisation tag</td>
<td>[0,1]</td>
<td>1.1</td>
<td>o ([28] only)</td>
</tr>
<tr>
<td></td>
<td>This request parameter indicates to the issuer whether you are willing to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>accept partial authorisation approval. Possible values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 – Full authorisation only (default)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 – Partial authorisation also accepted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b1</td>
<td>PAN – Primary Account Number</td>
<td>[0-9]</td>
<td>8,19</td>
<td>m</td>
</tr>
<tr>
<td>b3</td>
<td>Card expiration month</td>
<td>[0-9]</td>
<td>2,2</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Two-digit number (mm format)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b4</td>
<td>Card expiration year</td>
<td>[0-9]</td>
<td>2,2</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Two-digit number (yy format)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b5</td>
<td>Card Security Code (CVV / CVC) as printed on the card</td>
<td>[0-9]</td>
<td>3,3</td>
<td>m</td>
</tr>
<tr>
<td>b21</td>
<td>Passthrough wallet indicator</td>
<td>[A-Za-z\ ]</td>
<td>9-12</td>
<td>c (m if transaction was originally an Apple Pay, Google Pay or VTS/M4M transaction)</td>
</tr>
<tr>
<td></td>
<td>Indicates whether the transaction originally issued from a passthrough wallet supported by Credorax. Possible values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• applepay: for Apple Pay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• googlepay: for Google Pay</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• vts_mdes_token: for VTS and M4M (MDES for Merchants) token-based transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c1</td>
<td>Cardholder's full name</td>
<td>\ a-zA-Z]</td>
<td>5,45</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>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 recommended when initiating 3D secure transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c2</td>
<td>Cardholder's contact phone number</td>
<td>[0-9.]</td>
<td>5,32</td>
<td>o</td>
</tr>
<tr>
<td>c3</td>
<td>Cardholder's email address</td>
<td>email</td>
<td>7,64</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>This parameter should be transmitted as a valid email address such as <a href="mailto:joe@bloggs.com">joe@bloggs.com</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A default valid email address should always be transmitted in Card-Present transactions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>c4</td>
<td>Cardholder Billing Address street number</td>
<td>[0-9]</td>
<td>1,16</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>If the processor supports AVS then the transmission of this parameter will trigger the AVS system.</td>
<td></td>
<td></td>
<td>recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td></td>
<td>Note that the street number should be omitted from the c5 parameter if this parameter is transmitted.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c5</td>
<td>Cardholder Billing Address street name</td>
<td>[a-zA-Z0-9-]</td>
<td>4,50</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>The street number should not be included here if the c4 parameter is transmitted.</td>
<td></td>
<td></td>
<td>recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>c7</td>
<td>Cardholder Billing Address city name</td>
<td>[a-zA-Z-]</td>
<td>3,30</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>recommended – when initiating 3D secure transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>recommended – when initiating 3D secure transaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c9</td>
<td>Cardholder Billing Address Country Code</td>
<td>[A-Z]</td>
<td>2,2</td>
<td>c (required for [23], [28])</td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="https://www.iso.org/obp/ui#iso:std:iso:3166:1:en">ISO 3166-1-alpha-2</a> for a reference list.</td>
<td></td>
<td></td>
<td>recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td>c10</td>
<td>Cardholder Billing Address Postal/ZIP Code</td>
<td>[a-zA-Z0-9-]</td>
<td>1,9</td>
<td>c (required for [23], [28])</td>
</tr>
<tr>
<td></td>
<td>If transmitted, this value is sent to the issuer and will be part of the issuer's AVS checks</td>
<td></td>
<td></td>
<td>recommended – when initiating 3D secure transaction</td>
</tr>
<tr>
<td></td>
<td>Note: not all Payment Processors support AVS checks. Please refer to <a href="https://www.example.com">Source Payment Gateway: Processors Specification</a> for further details.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d1</td>
<td>Cardholder IP Address</td>
<td>[0-9.]</td>
<td>7,15</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>The IP address of the server that is connecting to the Source gateway should always be transmitted in Card-Present transactions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>d2</td>
<td>Echo parameter</td>
<td>Text</td>
<td>3,128</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f21</td>
<td>Boolean field specifying whether the fraud protection service check should be bypassed.</td>
<td>[0-1]</td>
<td>1,1</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>Send for a fraud check. (default value)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Do not send for a fraud check</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Only available to merchants using the Smart Guard fraud protection service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>f22</td>
<td>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.</td>
<td>[0-9]</td>
<td>0,4</td>
<td>o</td>
</tr>
<tr>
<td>h3</td>
<td>Sub-Merchant ID</td>
<td>[0-9]</td>
<td>1,15</td>
<td>c (Payment Facilitators)</td>
</tr>
<tr>
<td></td>
<td>The merchant ID of a sub-merchant belonging to a Payment Facilitator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to Source Payment Gateway: Processors Specification to learn which Payment Facilitators are supported.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number</td>
<td>Text</td>
<td>1,32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>This optional field is a secondary transaction reference number which can be sent alongside a1.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: No plaintext cardholder data should be provided in this field.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>h15</td>
<td>Seller Information</td>
<td>[a-zA-Z0-9</td>
<td>]</td>
<td>9,164</td>
</tr>
<tr>
<td></td>
<td>This field contains seller information. When using this field, &quot;Seller ID&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>is mandatory. The ID should be a unique identifier such as the seller name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or an internal registration number.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Populate these fields with the following information, delimited by &quot;</td>
<td>&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: This field is used by marketplaces.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Length (min, max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller ID</td>
<td>[a-zA-Z0-9</td>
<td>]</td>
<td>4,64</td>
<td></td>
</tr>
<tr>
<td>Seller country</td>
<td>[A-Z]</td>
<td>3,3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller city</td>
<td>[a-zA-Z</td>
<td>]</td>
<td>3,30</td>
<td></td>
</tr>
<tr>
<td>Seller street</td>
<td>[a-zA-Z0-9</td>
<td>]</td>
<td>4,50</td>
<td></td>
</tr>
<tr>
<td>Seller zip code</td>
<td>[a-zA-Z0-9</td>
<td>]</td>
<td>1,9</td>
<td></td>
</tr>
<tr>
<td>Seller state</td>
<td>[a-zA-Z0-9]</td>
<td>3,3</td>
<td></td>
<td></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</td>
<td>Text</td>
<td>1,39</td>
<td>o</td>
</tr>
</tbody>
</table>

The Descriptor that appears on the cardholder's statement.

Refer to Source 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.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Create Token Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>i8</td>
<td>3D Secure Data</td>
<td>[a-zA-Z0-9:]==+</td>
<td>10,128</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Compose of 3 different parameters delimited by a colon:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1. ECI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. CAVV/AAV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. XID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="#">Appendix J: How to provide 3D Secure Data on the i8 Parameter</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to <a href="#">Source Payment Gateway: Processors Specification</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A transmitted i8 will not be routed to Payment Processors that do not support this feature. Furthermore, the transaction will be rejected by the Source gateway if no optional Processor is found.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_version</td>
<td>Indicates the 3D Secure protocol version</td>
<td>[0-9]</td>
<td>3,5</td>
<td>c (m if using i8)</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.1.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.2.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_dstrxid</td>
<td>3DS Directory server transaction ID. Must be sent if 3ds_version = 2.0 or higher and i8 is used. Refer to <a href="#">Appendix J: How to Provide 3D Secure Data on the i8 Parameter</a></td>
<td>[0-9A-Za-z-]</td>
<td>34</td>
<td>c (m if 3ds_version = 2.0 or higher)</td>
</tr>
<tr>
<td>j1</td>
<td>Primary Account Recipient's date of birth</td>
<td>YYYYMMDD</td>
<td></td>
<td>c (6012 in UK)</td>
</tr>
<tr>
<td>j2</td>
<td>Masked PAN or account number from merchant systems.</td>
<td>[a-zA-Z0-9-]</td>
<td>8,8</td>
<td>c (6012 in UK)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>j3</td>
<td>Primary Account Recipient's Postal Code</td>
<td>[a-zA-Z0-9 /-]/</td>
<td>2,6</td>
<td>c (6012 in UK)</td>
</tr>
<tr>
<td>j4</td>
<td>Primary Account Recipient's partial surname</td>
<td>[a-zA-Z-]</td>
<td>2,6</td>
<td>c (6012 in UK)</td>
</tr>
<tr>
<td>j5</td>
<td>Funds Recipient’s First Name</td>
<td>[-“A-Za-z]</td>
<td>1,30</td>
<td>o</td>
</tr>
<tr>
<td>j6</td>
<td>Funds Recipient’s Street Address</td>
<td>[“0-9A-Za-z]</td>
<td>1,30</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Create Token Operations</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------</td>
<td>---------------</td>
<td>--------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>j7</td>
<td>Funds Recipient’s City</td>
<td>[“0-9A-Za-z”]</td>
<td>1.25</td>
<td>o</td>
</tr>
<tr>
<td>j8</td>
<td>Funds Recipient’s State/Province Code</td>
<td>[0-9A-Za-z]</td>
<td>2.3</td>
<td>o</td>
</tr>
<tr>
<td>j9</td>
<td>Funds Recipient’s Country Code</td>
<td>[A-Z]</td>
<td>3.3</td>
<td>o</td>
</tr>
<tr>
<td>j10</td>
<td>Funds Recipient’s Phone Number</td>
<td>[0-9-]</td>
<td>1.20</td>
<td>o</td>
</tr>
<tr>
<td>j11</td>
<td>Funds Recipient’s Date of Birth</td>
<td>MMDDYYYY</td>
<td>8.8</td>
<td>o</td>
</tr>
<tr>
<td>j12</td>
<td>Funds Recipient’s Postal Code</td>
<td>[a-zA-Z0-9-]</td>
<td>1.10</td>
<td>o</td>
</tr>
<tr>
<td>j13</td>
<td>Funds Recipient’s Surname</td>
<td>[A-Za-z]</td>
<td>1.30</td>
<td>o</td>
</tr>
<tr>
<td>r1</td>
<td>Chooses the Processor for the specific transaction</td>
<td>[a-zA-Z0-9-]</td>
<td>0.9</td>
<td>o</td>
</tr>
<tr>
<td>r2</td>
<td>Chooses the Processor MID for the specific transaction</td>
<td>[a-zA-Z0-9-]</td>
<td>0.32</td>
<td>o</td>
</tr>
<tr>
<td>r3</td>
<td>Routing sequence number</td>
<td>[1-9]</td>
<td>12</td>
<td>o</td>
</tr>
<tr>
<td>3ds_initiate</td>
<td>Indicates whether to initiate the Source 3D Secure</td>
<td>[0-3]</td>
<td>2.2</td>
<td>o (default value: 02)</td>
</tr>
<tr>
<td></td>
<td>Authentication process. Possible values are:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01: Initiate 3D Secure before completing the payment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02: Process payment without 3D Secure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03: Initiate 3D Secure according to the 3DS Adviser</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>result</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04: Only initiate the 3DS Adviser service. Relevant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>only for op code 98.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For additional information about the 3D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>secure process, see Appendix I: 3D Secure.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If the transaction contains both the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3ds_initiate parameter and the i8 parameter, the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transaction will be declined.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>token_eci</td>
<td>ECI value returned from the token decryption process</td>
<td>[0-9]</td>
<td>2.2</td>
<td>c (m if transaction is</td>
</tr>
</tbody>
</table>
Use Token Operations


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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Use Token Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>token_crypto</td>
<td>CAVV/AAV value returned from the token decryption process</td>
<td>[A-Za-z0-9]</td>
<td>40,40</td>
<td>[10] [23] [28]</td>
</tr>
<tr>
<td>K</td>
<td>Unique cipher used for authenticating requests</td>
<td>[0-9A-Za-z]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix A: Message Cipher for further details on generating the cipher.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Use Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code</td>
<td>[0-9]</td>
<td>1,3 m</td>
<td>[11] [12] [16] [24] [32]</td>
</tr>
<tr>
<td>a1</td>
<td>Request ID</td>
<td>[-0-9A-Za-z]</td>
<td>1,32 m</td>
<td></td>
</tr>
<tr>
<td>a2</td>
<td>Payment Source Type</td>
<td>[0-9]</td>
<td>1,2 o</td>
<td></td>
</tr>
<tr>
<td>a4</td>
<td>Requested Billing Amount</td>
<td>[0-9]</td>
<td>1,12 m (required for [11], [12], [24], [32]) o (optional for [23]) Not required for [16]</td>
<td></td>
</tr>
<tr>
<td>a5</td>
<td>Transaction Currency</td>
<td>[A-Z]</td>
<td>3,3 m</td>
<td></td>
</tr>
<tr>
<td>a6</td>
<td>Transaction date (local date of the transaction)</td>
<td>yyyyMMdd</td>
<td>6,6 o</td>
<td></td>
</tr>
<tr>
<td>a7</td>
<td>Transaction time (local time of the transaction)</td>
<td>HHmmss</td>
<td>6,6 o</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Use Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-------</td>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>a8</td>
<td>Merchant Invoice ID</td>
<td>text</td>
<td>1,16</td>
<td>o [11] [12] [16] [24] [32]</td>
</tr>
<tr>
<td></td>
<td>Only required for subscription transactions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a9</td>
<td>Transaction Type. Valid values are:</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o ([24], [32] only)</td>
</tr>
<tr>
<td>Value</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>First recurring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Subsequent recurring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Card-Only Validation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Straight Operation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Unscheduled Card-on-File transactions initiated by the merchant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Unscheduled Card-on-File transactions initiated by the cardholder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Card validations for an unscheduled Card-on-File</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• By default, the transaction type is considered a straight operation unless specified otherwise.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transmitting a9 with a value of 5 for Operation Code 23 will trigger a rejection response.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a10</td>
<td>Authorisation Type:</td>
<td>[1-2]</td>
<td>1,1</td>
<td>o ([12], [32] only)</td>
</tr>
<tr>
<td></td>
<td>1. Final Authorisation (default value)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Pre-Authorisation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transactions referring to Pre-Authorisations must include an a4 parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Use Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>a11</td>
<td>Multiple Capture tag</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o ([12],[32] only)</td>
</tr>
<tr>
<td></td>
<td>Indicates the number of expected Captures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Only supported in Card-not-Present transactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Default value is 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Max value is 98</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Min value is 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a14</td>
<td>Partial Authorisation tag</td>
<td>[0,1]</td>
<td>1,1</td>
<td>o ([12],[32] only)</td>
</tr>
<tr>
<td></td>
<td>This request parameter indicates to the issuer whether you are willing to accept partial authorisation approval. Possible values:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0 – Full authorisation only (default)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 – Partial authorisation also accepted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d1</td>
<td>Cardholder’s IP Address</td>
<td>[0-9.]</td>
<td>7,15</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>The IP address of the server that is connecting to the Source Gateway should always be sent for Card-Present transactions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d2</td>
<td>Echo parameter</td>
<td>Text</td>
<td>3,128</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Any value up to 128 bytes long transmitted within a request will be returned within the response to this parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: No plaintext cardholder data should be provided in this field.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g1</td>
<td>Token</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>Source-generated Token that refers to a stored card profile.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Use Token Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>g6</td>
<td>Initial transaction ID</td>
<td>[0-9A-Za-z]</td>
<td>13,15</td>
<td>o (m if a9=2 or 8)</td>
</tr>
<tr>
<td></td>
<td>The z50 parameter that was received in the original transaction response. Must be sent to ensure the transaction is considered an MIT transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the transaction is an MIT and the original transaction was prior to 14 Sept. 2019, send the following value: 9999999999999999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> As of 1 April 2022 Visa requires that each subsequent transaction includes a proper 'initial transaction id' on the g6 parameter. The generic value above will no longer be accepted. This applies to all transactions including those initiated before September 2019. If you do not have this value, work with your customers to get a new original transaction authorised and authenticated.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number</td>
<td>Text</td>
<td>1,32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>This optional field is a secondary transaction reference number which can be transmitted alongside an a1 parameter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> No plaintext cardholder data should be provided in this field.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length (min, max)</td>
<td>Use Token Operations</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>h15</td>
<td>Seller Information&lt;br&gt;This field contains seller information. When using this field, &quot;Seller ID&quot; 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 &quot;</td>
<td>&quot;.&lt;br&gt;&lt;br&gt;Note: This field is used by marketplaces.</td>
<td>[a-zA-Z0-9-|]</td>
<td>9,164</td>
</tr>
<tr>
<td>i2</td>
<td>Billing Descriptor&lt;br&gt;The Descriptor that appears on the cardholder's statement.&lt;br&gt;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</td>
<td>Text</td>
<td>1,39</td>
<td>o (Not required for [16])</td>
</tr>
<tr>
<td>j5</td>
<td>Funds Recipient's First name&lt;br&gt;[&quot;A-Za-z]</td>
<td>1,30</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j6</td>
<td>Funds Recipient's Street Address&lt;br&gt;[&quot;0-9A-Za-z]</td>
<td>1,30</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j7</td>
<td>Funds Recipient's City&lt;br&gt;[&quot;0-9A-Za-z]</td>
<td>1,25</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j8</td>
<td>Funds Recipient's State/Province Code&lt;br&gt;[0-9A-Za-z]</td>
<td>2,3</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j9</td>
<td>Funds Recipient's Country Code&lt;br&gt;[A-Z]</td>
<td>3,3</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j10</td>
<td>Funds Recipient's Phone Number&lt;br&gt;[0-9-]</td>
<td>1,20</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j11</td>
<td>Funds Recipient's Date of Birth&lt;br&gt;MMDDYYYY</td>
<td>8,8</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>j12</td>
<td>Funds Recipient's Postal Code&lt;br&gt;[a-zA-Z0-9-]</td>
<td>1,10</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Use Token Operations</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------</td>
<td>-------------</td>
<td>--------</td>
<td>----------------------</td>
</tr>
<tr>
<td>3ds_initiate</td>
<td>Indicates whether to initiate the Source 3D Secure Authentication process. Possible values are: 01: Initiate 3D Secure before completing the payment 02: Process payment without 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</td>
<td>[0-3]</td>
<td>2,2</td>
<td>o (default value: 02)</td>
</tr>
</tbody>
</table>
Referral Token Operations

[13] Use Token – Capture
This operation generates a Capture [3] that pertains to a previous operation [12] transaction.

Condition: 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

Condition: 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

Condition: 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.

Condition: 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

Condition: Can only be transmitted if a previous [32] operation has already been transmitted.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Referral Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Source assigned Gateway Merchant ID</td>
<td>[A-Z0-9_]</td>
<td>3.6</td>
<td>[13] [14] [15] [29] [33]</td>
</tr>
<tr>
<td>K</td>
<td>Unique cipher for authenticating requests Refer to Appendix A: Message Cipher for further details on generating the cipher.</td>
<td>[0-9A-Za-z]</td>
<td>1.32</td>
<td>m</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code The operation code is used for determining the requested service. See the list in Referral Token Operations.</td>
<td>[0-9]</td>
<td>1.3</td>
<td>m</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Referral Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>---------------------</td>
</tr>
<tr>
<td>a1</td>
<td>Request ID</td>
<td>[-0-9A-Za-z]</td>
<td>1,32</td>
<td>m [13] [14] [15] [29] [33]</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a2</td>
<td>Payment Source Type</td>
<td>[0-9]</td>
<td>1,2</td>
<td>o [7]</td>
</tr>
<tr>
<td></td>
<td>Valid options are: 2 Online Order (default value) 3 Telephone Order 4 Mail Order 5 Virtual Terminal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a4</td>
<td>Requested Billing Amount</td>
<td>[0-9]</td>
<td>1,12</td>
<td>o [10]</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a5</td>
<td>Presentment Currency</td>
<td>[A-Z]</td>
<td>3,3</td>
<td>o [12]</td>
</tr>
<tr>
<td></td>
<td>Indicates the presentment currency that should be used in the transaction (every currency used must be preconfigured on the Source platform). Refer to ISO 4217-alpha-3 for more details</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a6</td>
<td>Transaction date (local date of the transaction)</td>
<td>yyMMdd</td>
<td>6,6</td>
<td>o [10]</td>
</tr>
<tr>
<td>a7</td>
<td>Transaction time (local time of the transaction)</td>
<td>HHmmss</td>
<td>6,6</td>
<td>o [10]</td>
</tr>
</tbody>
</table>
### Name: Transaction Type. Valid values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>First recurring</td>
</tr>
<tr>
<td>2</td>
<td>Subsequent recurring</td>
</tr>
<tr>
<td>5</td>
<td>Card-Only Validation</td>
</tr>
<tr>
<td>6</td>
<td>Straight Operation</td>
</tr>
<tr>
<td>8</td>
<td>Unscheduled Card-on-File transactions initiated by the merchant</td>
</tr>
<tr>
<td>9</td>
<td>Unscheduled Card-on-File transactions initiated by the cardholder</td>
</tr>
<tr>
<td>10</td>
<td>Card validations for an unscheduled Card-on-File</td>
</tr>
</tbody>
</table>

**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.

### Name: Final capture indication. In multiple-capture scenarios, use this parameter to indicate whether this capture is the final capture. Valid values are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Final capture</td>
</tr>
<tr>
<td>0</td>
<td>Not final capture</td>
</tr>
</tbody>
</table>

### Name: Card expiration month

Two-digit number (mm format)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0-9]</td>
<td>1.1</td>
</tr>
</tbody>
</table>

### Name: Card expiration year

Two-digit number (yy format)

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0-9]</td>
<td>2.2</td>
</tr>
</tbody>
</table>

### Name: Cardholder IP Address

The IP Address of the server that is connecting to the **Source** gateway should always be sent in Card-Present transactions.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Referral Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>d2</td>
<td>Echo parameter</td>
<td>Text</td>
<td>3,128</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g1</td>
<td>Token</td>
<td>[a-zA-Z0-9]</td>
<td>1.32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>A Source-generated Token that references a stored card profile.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g2</td>
<td>Response ID</td>
<td>[a-zA-Z0-9]</td>
<td>1.32</td>
<td>m</td>
</tr>
<tr>
<td></td>
<td>The z1 parameter from a corresponding past transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g3</td>
<td>Authorisation Code</td>
<td>[a-zA-Z0-9]</td>
<td>1.10</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>The z4 parameter from a corresponding past transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g4</td>
<td>Request ID</td>
<td>[0-9A-Za-z]</td>
<td>1.32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>The a1 parameter from a corresponding past transaction.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>g6</td>
<td>Initial transaction ID</td>
<td>[0-9A-Za-z]</td>
<td>13.15</td>
<td>o (m if a9=2 or 8)</td>
</tr>
<tr>
<td></td>
<td>The z50 parameter that was received in the original transaction response. Must be sent to ensure the transaction is considered an MIT transaction. If the transaction is an MIT and the original transaction was prior to 14 Sept. 2019, send the following value: 9999999999999999</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> As of 1 April 2022 Visa requires that each subsequent transaction includes a proper 'initial transaction id' on the g6 parameter. The generic value above will no longer be accepted. This applies to all transactions including those initiated before September 2019. If you do not have this value, work with your customers to get a new original transaction authorised and authenticated.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number</td>
<td>Text</td>
<td>1.32</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
<td>Referral Operations</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>---------------------</td>
</tr>
<tr>
<td>h15</td>
<td>Seller Information</td>
<td>[a-zA-Z0-9-|]</td>
<td>9,164</td>
<td>o ([13], [29], [33] only)</td>
</tr>
<tr>
<td></td>
<td>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 “</td>
<td>”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This field is used by marketplaces.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Type</td>
<td>Length (min, max)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller ID</td>
<td>[a-zA-Z0-9-|]</td>
<td>4,64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller country</td>
<td>[A-Z]</td>
<td>3,3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller city</td>
<td>[a-zA-Z-]</td>
<td>3,30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller street</td>
<td>[a-zA-Z0-9-|]</td>
<td>4,50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller zip code</td>
<td>[a-zA-Z0-9-|]</td>
<td>1,9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Seller state</td>
<td>[a-zA-Z0-9-]</td>
<td>3,3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1</td>
<td>Transaction Free Text Description</td>
<td>Text</td>
<td>5,64</td>
<td>o</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Operation Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[34]</td>
<td>Referral CFT (Credit Fund Transfer)</td>
</tr>
<tr>
<td>[35]</td>
<td>Independent CFT (Credit Fund Transfer)</td>
</tr>
<tr>
<td>[37]</td>
<td>Create Independent CFT Token</td>
</tr>
<tr>
<td>[38]</td>
<td>Use Independent CFT Token</td>
</tr>
<tr>
<td>[98]</td>
<td>Authenticate Cardholder without payment (3D Secure)</td>
</tr>
<tr>
<td>[88]</td>
<td>Create Token and Authenticate Cardholder without payment (3D Secure)</td>
</tr>
<tr>
<td>[89]</td>
<td>Use Token and Authenticate Cardholder without payment (3D Secure)</td>
</tr>
</tbody>
</table>

**[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 Credorax; 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).

**Condition:** The original transaction that is referred to must be successfully authorised and captured in order to process a [34] - Referral 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 Credorax; 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 scheme's rules, the payout transactions are final and cannot be voided (except for Mastercard transactions with the MCC 7995).

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

- [34] – Referral CFT
- [35] – Independent CFT
- [37] – Create token – Independent CFT
- [38] – Use token – Independent CFT

Attempting to void these transactions 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 Source 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 Source 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 Source 3D Secure service without initiating a payment.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Referral CFT [34]</th>
<th>Independent CFT [35], [37]</th>
<th>Use Independent CFT Token [38]</th>
<th>3D Only [98]</th>
<th>Create Token 3D Only [88]</th>
<th>Use Token 3D Only [89]</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Merchant ID</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>K</td>
<td>Package Signature</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Referral CFT [34]</td>
<td>Independent CFT [35], [37]</td>
<td>Use Independent CFT Token [38]</td>
<td>3D Only [98]</td>
<td>Create Token 3D Only [88]</td>
<td>Use Token 3D Only [89]</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>--------------------------------</td>
<td>--------------</td>
<td>---------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>a1 Request ID</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>a2 Source Type ID</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>a4 Billing Amount</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>a5 Billing Currency Code</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>a6 Transaction Date</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>a7 Transaction Time</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>a8 Merchant Order ID/Invoice</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>b1 Card Number</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>m</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>b3 Card Expiration Month (mm)</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>m</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>b4 Card Expiration Year (yy)</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>m</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c1 Billing Contact Name</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>m</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c2 Billing Contact Phone Number</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c3 Billing Email Address</td>
<td>m</td>
<td>-</td>
<td>-</td>
<td>m</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c4 Billing Street Number</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c5 Billing Street Name</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c7 Billing City Name</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c8 Billing Territory ISO Code</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c9 Billing Country ISO Code</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>c10 Billing Postal Code</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>d1 End User IP Address</td>
<td>o</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>d2 Echo</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>g1 Credorax assigned Token id</td>
<td>-</td>
<td>-</td>
<td>m</td>
<td>o</td>
<td>-</td>
<td>m</td>
<td>-</td>
</tr>
<tr>
<td>g2 Previous Response ID</td>
<td>m</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>g3 Previous Authorisation Code</td>
<td>o</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>g4 Previous Request ID</td>
<td>o</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>g6 Initial transaction ID</td>
<td>o</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Referral CFT [34]</td>
<td>Independent CFT [35], [37]</td>
<td>Use Independent CFT Token [38]</td>
<td>3D Only [98]</td>
<td>Create Token 3D Only [88]</td>
<td>Use Token 3D Only [89]</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>--------------</td>
<td>----------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number</td>
<td>o o o</td>
<td>o o o</td>
<td>o o o</td>
<td>o o o</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1</td>
<td>Transaction Free Text Description</td>
<td>o o -</td>
<td>o o o</td>
<td>- o o</td>
<td>o o o</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i2</td>
<td>Statement Charge Descriptor</td>
<td>- - -</td>
<td>- o o</td>
<td>o o o</td>
<td>o o o</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j5</td>
<td>Funds Recipient's First Name</td>
<td>c (m if was not sent on the original transaction)</td>
<td>m m</td>
<td>- - -</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j6</td>
<td>Funds Recipient's Street Address</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j7</td>
<td>Funds Recipient's City</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j8</td>
<td>Funds Recipient's State/Province Code</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j9</td>
<td>Funds Recipient's Country Code</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>m (when j9=CAN)</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j10</td>
<td>Funds Recipient's Phone Number</td>
<td>o o o</td>
<td>o o o</td>
<td>- - -</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j11</td>
<td>Funds Recipient's Date of Birth</td>
<td>o o o</td>
<td>o o o</td>
<td>- - -</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j12</td>
<td>Funds Recipient's Postal Code</td>
<td>o o o</td>
<td>o o o</td>
<td>- - -</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>j13</td>
<td>Funds Recipient's Surname</td>
<td>c (m if was not sent on the original transaction)</td>
<td>m m</td>
<td>- - -</td>
<td>- - -</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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 Source 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 Source'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 Source 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Retrieval Operation [101]</th>
<th>Get Fraud Scoring [103]</th>
<th>Get Fast Funds Indicator [104]</th>
<th>Use Token Get Fast Funds Indicator [105]</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Merchant ID</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>K</td>
<td>Package Signature</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>a1</td>
<td>Request ID</td>
<td>m</td>
<td>m</td>
<td>m</td>
<td>m</td>
</tr>
<tr>
<td>a2</td>
<td>Source Type ID</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>a4</td>
<td>Billing Amount</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>a5</td>
<td>Billing Currency Code</td>
<td>o</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>a6</td>
<td>Transaction Date</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>a7</td>
<td>Transaction Time</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>a8</td>
<td>Merchant Order ID/Invoice</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>b1</td>
<td>Card Number</td>
<td>-</td>
<td>m</td>
<td>m</td>
<td>-</td>
</tr>
<tr>
<td>b3</td>
<td>Card Expiration Month (mm)</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>b4</td>
<td>Card Expiration Year (yy)</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c1</td>
<td>Billing Contact Name</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c2</td>
<td>Billing Contact Phone Number</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c3</td>
<td>Billing Email Address</td>
<td>-</td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c4</td>
<td>Billing Street Number</td>
<td>-</td>
<td>c</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c5</td>
<td>Billing Street Name</td>
<td>-</td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Retrieval Operation [101]</td>
<td>Get Fraud Scoring [103]</td>
<td>Get Fast Funds Indicator [104]</td>
<td>Use Token Get Fast Funds Indicator [105]</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------------------</td>
<td>---------------------------</td>
<td>-------------------------</td>
<td>-------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>c7</td>
<td>Billing City Name</td>
<td></td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c8</td>
<td>Billing Territory ISO Code</td>
<td></td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c9</td>
<td>Billing Country ISO Code</td>
<td></td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>c10</td>
<td>Billing Postal Code</td>
<td></td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>d1</td>
<td>End User IP Address</td>
<td></td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>d2</td>
<td>Echo</td>
<td></td>
<td>o</td>
<td>o</td>
<td>-</td>
</tr>
<tr>
<td>g1</td>
<td>Credorax assigned Token id</td>
<td></td>
<td>-</td>
<td>-</td>
<td>m</td>
</tr>
<tr>
<td>g2</td>
<td>Previous Response ID</td>
<td></td>
<td>c</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>g3</td>
<td>Previous Authorisation Code</td>
<td></td>
<td>m</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>g4</td>
<td>Previous Request ID</td>
<td></td>
<td>m</td>
<td>o</td>
<td>-</td>
</tr>
<tr>
<td>g6</td>
<td>Initial transaction ID</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>h3</td>
<td>Sub merchant id</td>
<td></td>
<td>-</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number</td>
<td></td>
<td>o</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>i1</td>
<td>Transaction Free Text Description</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>i2</td>
<td>Statement Charge Descriptor</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j5</td>
<td>Funds Recipient's First Name</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j6</td>
<td>Funds Recipient's Street Address</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j7</td>
<td>Funds Recipient's City</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j8</td>
<td>Funds Recipient's State/Province Code</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j9</td>
<td>Funds Recipient's Country Code</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j10</td>
<td>Funds Recipient's Phone Number</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j11</td>
<td>Funds Recipient's Date of Birth</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j12</td>
<td>Funds Recipient's Postal Code</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>j13</td>
<td>Funds Recipient's Surname</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Retrieval Operation [101]</td>
<td>Get Fraud Scoring [103]</td>
<td>Get Fast Funds Indicator [104]</td>
<td>Use Token Get Fast Funds Indicator [105]</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------------------</td>
<td>---------------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>3ds_initiate</td>
<td>Indicates whether to initiate the Source 3D Secure Authentication process. Possible values are:</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>01: Initiate 3D Secure before completing the payment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02: Process payment without 3D Secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03: Initiate 3D Secure according to the 3DS Adviser result</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04: Only initiate the 3DS Adviser service. Relevant only for op code 98.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For additional information about the 3D Secure process, see Appendix I: 3D Secure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: If the transaction contains both the 3ds_initiate parameter and the i8 parameter, the transaction will be declined.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 parameters may be added in the future without prior notice. Make sure your implementation can support that.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Source-assigned Gateway Merchant ID</td>
<td>[A-Z0-9_]</td>
<td>3,6</td>
</tr>
<tr>
<td>T</td>
<td>Transaction processing timestamp formatted as MM/dd/yyyy HH:mm:ss</td>
<td>timestamp</td>
<td>1,32</td>
</tr>
<tr>
<td>a1</td>
<td>Request ID as sent in the request</td>
<td>[-0-9A-Za-z]</td>
<td>1,32</td>
</tr>
<tr>
<td>a2</td>
<td>Payment Source Type as sent in the request</td>
<td>[0-9]</td>
<td>1,2</td>
</tr>
<tr>
<td>a4</td>
<td>Requested Billing Amount as sent in the request</td>
<td>[0-9]</td>
<td>1,12</td>
</tr>
<tr>
<td>a6</td>
<td>Transaction date (local date of the transaction) as sent in the request</td>
<td>yyMMdd</td>
<td>6,6</td>
</tr>
<tr>
<td>a7</td>
<td>Transaction time (local time of the transaction) as sent in the request</td>
<td>HHmmss</td>
<td>6,6</td>
</tr>
<tr>
<td>a9</td>
<td>Transaction Type as sent in the request</td>
<td>[0,9]</td>
<td>1,2</td>
</tr>
<tr>
<td>b1</td>
<td>PAN – Primary Account Number. Masked as: #######****####</td>
<td>[0-9]</td>
<td>8,19</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>b2</td>
<td>Card type. Valid options are:</td>
<td>[0-9]</td>
<td>1,2</td>
</tr>
<tr>
<td></td>
<td><strong>Code</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Card Scheme</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Visa</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Mastercard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>American Express</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Isracard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Maestro</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>JCB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Discover</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Diners</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Cartes Bancaires</td>
<td></td>
</tr>
<tr>
<td>b3</td>
<td>Card expiration month as sent in the request</td>
<td>[0-9]</td>
<td>2,2</td>
</tr>
<tr>
<td>b4</td>
<td>Card expiration year as sent in the request</td>
<td>[0-9]</td>
<td>2,2</td>
</tr>
<tr>
<td>b20</td>
<td>Payment Account Reference (PAR)</td>
<td>[a-zA-Z0-9]</td>
<td>29,29</td>
</tr>
<tr>
<td>c1</td>
<td>Cardholder's full name as sent in the request</td>
<td>\ a-zA-Z</td>
<td>5,45</td>
</tr>
<tr>
<td>d2</td>
<td>Echo parameter as sent in the request</td>
<td>Text</td>
<td>3,128</td>
</tr>
<tr>
<td>g1</td>
<td>Token</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
</tr>
<tr>
<td></td>
<td>Source-generated Token that refers to a stored card profile.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>g2</td>
<td>Response ID as sent in the request</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
</tr>
<tr>
<td>h3</td>
<td>Sub-Merchant ID as sent in the request</td>
<td>0-9</td>
<td>1,15</td>
</tr>
<tr>
<td>h9</td>
<td>Merchant Reference Number as sent in the request</td>
<td>Text</td>
<td>1,32</td>
</tr>
<tr>
<td>i1</td>
<td>Transaction Free Text Description as sent in the request</td>
<td>Text</td>
<td>5,64</td>
</tr>
<tr>
<td>j1</td>
<td>Primary Account Recipient's date of birth as sent in the request</td>
<td>YYYYMMD D</td>
<td>8,8</td>
</tr>
<tr>
<td>j2</td>
<td>Masked PAN or account number from merchant systems as sent in the request</td>
<td>[a-zA-Z0-9-]</td>
<td>8,8</td>
</tr>
<tr>
<td>j3</td>
<td>Primary Account Recipient's Postal Code as sent in the request</td>
<td>[a-zA-Z0-9-/]</td>
<td>2,6</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>j4</td>
<td>Primary Account Recipient’s partial surname as sent in the request</td>
<td>[a-zA-Z]</td>
<td>2,6</td>
</tr>
<tr>
<td>z1</td>
<td>Source Gateway Transaction ID</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
</tr>
<tr>
<td></td>
<td>The Transaction ID that uniquely identifies this transaction in the Source gateway.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z2</td>
<td>Gateway Response Code.</td>
<td>[0-9]</td>
<td>1,3</td>
</tr>
<tr>
<td></td>
<td>A value of 05 means that the transactions were rejected by the processor. Refer to z6 to see the original response code</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to Appendix B: Operation Result Codes for more information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z3</td>
<td>Description of the operation’s result</td>
<td>text</td>
<td>5,256</td>
</tr>
<tr>
<td>z4</td>
<td>Authorisation Code</td>
<td>[a-zA-Z0-9]</td>
<td>1,10</td>
</tr>
<tr>
<td>z5</td>
<td>Risk Score</td>
<td>[ABC0-9]</td>
<td>1,6</td>
</tr>
<tr>
<td></td>
<td>The fraud protection service’s response. The transaction will be 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Refer to SmartGuard for more information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z6</td>
<td>Processing Response Reason Code. The original Processor response is provided in parameter z41.</td>
<td>[A-Z0-9]</td>
<td>1,3</td>
</tr>
<tr>
<td></td>
<td>For more information, refer to Appendix D: Processing Response Reason Codes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z9</td>
<td>AVS response</td>
<td>[A-Z0-9]</td>
<td>1,2</td>
</tr>
<tr>
<td></td>
<td>The Address Verification Service (AVS) Authorisation response provided by the acquirer at the time of Authorisation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information, refer to Appendix C: AVS Response Codes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z13</td>
<td>RRN</td>
<td>[a-zA-Z0-9]</td>
<td>1,32</td>
</tr>
<tr>
<td></td>
<td>The transaction Retrieval Reference Number (RRN) may be provided by the processor as an additional identifier of the transaction.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>z14</td>
<td>CVV2 response code</td>
<td>[A-Z]</td>
<td>1,1</td>
</tr>
<tr>
<td></td>
<td>Valid values are:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'M' - CVV2/CVC2 Matches</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'N' - CVV2/CVC2 does not Match</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'P' - Not processed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'S' - The CVV2 should be on the card but the merchant indicates it is not.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'U' - CVV2/CVC2 Unavailable – issuer does not support this parameter</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Y' - CVC1 Incorrect</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'1' - CVV2/CVC2 Unavailable – processor / card type does not support this parameter</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'2' - An unrecognised result code was returned by the processor</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'3' - No result code was returned by the processor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z15</td>
<td>Approved Billing Amount</td>
<td>[0-9]</td>
<td>1.10</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z16</td>
<td>Balance Response. For Card-Present transactions carried out with debit or prepaid 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.</td>
<td>[0-9]</td>
<td>1,10</td>
</tr>
<tr>
<td>z17</td>
<td>Balance Response Currency. If a balance response is provided (see notes relating to field z16 above), its currency will be returned in this parameter.</td>
<td>[A-Z0-9]</td>
<td>3,3</td>
</tr>
<tr>
<td>z21</td>
<td>Indicates the result of the transaction’s transmission to the fraud-protection service.</td>
<td>[0-9-]</td>
<td>1,3</td>
</tr>
<tr>
<td></td>
<td>See <a href="#">Appendix E: z21 Possible Values</a> for the list of all possible z21 result codes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>z25</td>
<td>Indicates the updated amount of the transaction. Populated only in cases of changed amount such as authorisation void and incremental authorisation.</td>
<td>[0-9-]</td>
<td>1.12</td>
</tr>
<tr>
<td>z30</td>
<td>Indicates the Processor Routing Method used for the transaction. Optional values are:</td>
<td>[0-9]</td>
<td>1,1</td>
</tr>
<tr>
<td></td>
<td>1 Routing parameter (r1 or r2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 Routing rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 Processor priority</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>z31</td>
<td>The Processor Routing Rule ID that was responsible for the routing decision. Only populated in cases where z30=2.</td>
<td>[0-9]</td>
<td>0,4</td>
</tr>
<tr>
<td>z33</td>
<td>The Payment Processor processed the transaction.</td>
<td>[A-Z]</td>
<td>1,255</td>
</tr>
<tr>
<td>z34</td>
<td>The Payment Processor MID.</td>
<td>[a-zA-Z0-9]</td>
<td>1,255</td>
</tr>
<tr>
<td>z35</td>
<td>Indicates whether Smart Routing reroute is applied to this transaction.</td>
<td>Boolean</td>
<td>4,5</td>
</tr>
</tbody>
</table>
| 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 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-zA-Z0-9] | 1,255 |
<p>| 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 |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>z43</td>
<td>Indicates whether the transaction was handled by the Credorax stand-in service as well as the transaction status. Possible values are: 1 Transaction pending Credorax stand-in service 2 Credorax stand-in service final response 3 Transaction does not meet Credorax stand-in max aggregated transaction amount threshold 4 Transaction does not meet Credorax stand-in max transaction amount threshold 5 Unable to get final answer from the connector / processor. Credorax stand-in service terminated for this transaction</td>
<td>[0-9]</td>
<td>1</td>
</tr>
<tr>
<td>Z44</td>
<td>Merchant Advice Code (MAC) Indicates whether an attempt to retry the transaction is advised. Possible values are: 01: Updated or additional information is needed 02: Try again later 03: Do not try again 04: Token requirements not fulfilled for this token type 21: Payment cancelation</td>
<td>[0-9]</td>
<td>2</td>
</tr>
<tr>
<td>z50</td>
<td>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).</td>
<td>[a-zA-Z0-9]</td>
<td>13,15</td>
</tr>
<tr>
<td>z51</td>
<td>Fast funds indicator. Indicates whether the issuer supports fast funds functionality. Y - Supports fast funds for domestic &amp; cross-border payments C - Supports fast funds for cross-border payments D - Supports fast funds for domestic payments N - No result</td>
<td>[A-Z]</td>
<td>1,1</td>
</tr>
<tr>
<td>z55</td>
<td>Payment ID. A unique transaction identifier that accompanies all transactions related to the same purchase.</td>
<td>[a-zA-Z0-9]</td>
<td>32,32</td>
</tr>
<tr>
<td>3ds_eci</td>
<td>The ECI assigned to the authentication</td>
<td>[0-9]</td>
<td>1,2</td>
</tr>
<tr>
<td>3ds_cavv</td>
<td>The authentication value received from the issuer</td>
<td>[a-zA-Z0-9]</td>
<td>0,64</td>
</tr>
<tr>
<td>3ds_trxid</td>
<td>The assigned 3D transaction ID</td>
<td>[a-zA-Z0-9]</td>
<td>36,36</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>3ds_xid</td>
<td>XID generated as part of the authentication. Relevant only for 3D Secure version 1.0.2</td>
<td>[a-zA-Z0-9]</td>
<td>28,28</td>
</tr>
<tr>
<td>3ds_status</td>
<td>The result of the authentication process. Possible values:</td>
<td>[A-Z]</td>
<td>1,1</td>
</tr>
<tr>
<td></td>
<td>A - Attempts Processing Performed; Not Authenticated/Verified, but a proof of attempted authentication/verification is provided</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Y - Authentication/Account Verification Successful</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>N - Not Authenticated/Account Not Verified; Transaction denied</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C - Challenge Required; Additional authentication is required</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R - Authentication/Account Verification Rejected; Issuer is rejecting authentication/verification and requests that authorisation not be attempted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>U - Authentication/Account Verification Could Not Be Performed, Technical or other problem</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>I - Informational Only; Merchant challenge preference acknowledged.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D - Challenge Required; Decoupled Authentication confirmed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_valid_payment</td>
<td>Credorax recommendation whether to initiate payment following the authentication results.</td>
<td>Boolean</td>
<td>1,1</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>y - yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>n - no</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_version</td>
<td>Indicates the 3D Secure protocol version</td>
<td>[0-9]</td>
<td>3.5</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_acsurl</td>
<td>The received issuer URL for the authentication process</td>
<td>[a-zA-Z0-9]</td>
<td>0,2048</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>Length</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>--------</td>
</tr>
<tr>
<td>3ds_pareq</td>
<td>Relevant only for 3D secure 1.0 flows. Used when accessing the 3ds_acsurl</td>
<td>[a-zA-Z0-9]</td>
<td>0,2048</td>
</tr>
<tr>
<td>3ds_acstrxid</td>
<td>Unique transaction identifier assigned by the ACS to identify a single 3D secure transaction.</td>
<td>[a-zA-Z0-9]-.]</td>
<td>36,36</td>
</tr>
</tbody>
</table>
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 $M, O, c_1, c_{11}, c_2, h_8, h_9, i_{10}, i_4, ...$:
   a. Numbers
   b. Capital letters
   c. Small letters

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

Example: $3ds\_initiate, 3ds\_version, M, O, c_1, c_{11}, c_2, h_8, h_9, i_{10}, i_4, ...$

2. Replace the special characters $<>", \(, \backslash$ with spaces in each parameter value.
3. Remove any leading and trailing spaces in each parameter value.
4. Line up all parameter values in the same order.
5. Append the merchant’s unique signature key (provided in the connectivity details) to the value list.
6. Calculate the SHA256 hash of the sorted value set.
7. Include the resulting 64-character string as the request’s K parameter.

Signature Calculation Example

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

$$M=8632876&O=1&a_1=7894654&a_4=1099&b_1=4545454545454545&b_2=1&b_3=08&b_4=11&b_5=003&c_1=John\text{Smith}&c_3=johnsmith@yahoo.com&c_{10}=AB12DE&d_1=111.222.0.101$$

1. Sort the parameters:
   $$M, O, a_1, a_4, b_1, b_2, b_3, b_4, b_5, c_1, c_{10}, c_3, d_1$$
2. Replace any special characters $<>", \(, \backslash$ with spaces in each parameter value.
3. Remove any leading and trailing spaces in each parameter value.
4. Line up the values:
   $$863287617894654109945454545454545451099454545454545454510811003John\text{Smith}AB12DEjohnsmith@yahoo.com111.222.0.101$$
5. Append the signature key exactly as it appears in your connectivity details:
   86328761789465410994545454545454510811003John SmithAB1
   2DEjohnsmith@yahoo.com111.222.0.101SIGNKEY1

6. Calculate the SHA256 hash of the sorted value set:
   8f03b86acd09da945e367e9f73151252cfc59a3c27ad8402b6e543c948232f

7. Include the signature into the request query string:
   K=8f03b86acd09da945e367e9f73151252cfc59a3c27ad8402b6e543c948232f&M=86328
   76&O=1&a1=7894654&a4=1099&b1=4545454545454545&b2=1&b3=08&b4=11&b5=003
   &c1=John Smith&c10=AB1 2DE&c3=johnsmith@yahoo.com&d1=111.222.0.101

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

Response Signature

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

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

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-69</td>
<td>Transaction has been declined. Invalid 3ds_version parameter.</td>
</tr>
<tr>
<td>-68</td>
<td>Authentication process timed out. Please try again.</td>
</tr>
<tr>
<td>-66</td>
<td>Invalid combination of 3ds_initiate and exemption_action values</td>
</tr>
<tr>
<td>-65</td>
<td>Gateway MID is not allowed for this exemption</td>
</tr>
<tr>
<td>-64</td>
<td>TRA exemption is not allowed for this transaction amount</td>
</tr>
<tr>
<td>-63</td>
<td>The requested gateway mid is not enrolled to 3D-secure service.</td>
</tr>
<tr>
<td>-50</td>
<td>An error occurred during the 3D secure process</td>
</tr>
<tr>
<td>-39</td>
<td>You need to be registered with the 3D Adviser service to complete the request</td>
</tr>
<tr>
<td>-38</td>
<td>The transaction has been denied by the Gateway because 3D secure Authentication failed. Reason: {}</td>
</tr>
<tr>
<td>-37</td>
<td>Transaction has been denied. Malformed or missing {} parameter. Originating component: {}</td>
</tr>
<tr>
<td>-36</td>
<td>The selected Processor does not support some of the transaction's parameters.</td>
</tr>
<tr>
<td>-35</td>
<td>The selected MID is not registered to your account.</td>
</tr>
<tr>
<td>-33</td>
<td>You need to be registered with the routing service to complete the routing request.</td>
</tr>
<tr>
<td>-32</td>
<td>You are not registered with the selected Processor.</td>
</tr>
<tr>
<td>-30</td>
<td>Transaction Failed due to error in 3D secure process</td>
</tr>
<tr>
<td>-20</td>
<td>Processor authentication error. Please contact Credorax support.</td>
</tr>
<tr>
<td>-17</td>
<td>Fraud-protection service is unavailable</td>
</tr>
<tr>
<td>-16</td>
<td>Rejected. Overriding the fraud threshold is not allowed</td>
</tr>
<tr>
<td>-15</td>
<td>Rejected. Bypassing the fraud service is not allowed.</td>
</tr>
<tr>
<td>-13</td>
<td>The requested gateway mid is not enrolled in the 3D Secure Adviser service.</td>
</tr>
<tr>
<td>-12</td>
<td>Transaction has been declined due to security restrictions.</td>
</tr>
<tr>
<td>-11</td>
<td>Rejected. Format Error</td>
</tr>
<tr>
<td>-10</td>
<td>Internal server error. Please contact Source support.</td>
</tr>
<tr>
<td>-9</td>
<td>The parameter is malformed.</td>
</tr>
<tr>
<td>-8</td>
<td>The Package Signature is malformed.</td>
</tr>
<tr>
<td>-7</td>
<td>Incorrect Gateway Response. Connection is broken.</td>
</tr>
<tr>
<td>0</td>
<td>The transaction has been executed successfully.</td>
</tr>
<tr>
<td>1</td>
<td>The transaction has been denied by the Gateway.</td>
</tr>
</tbody>
</table>

Note: The “Reason” part is optional and may appear according to detected reason.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>The transaction has been denied by the Gateway due to its high fraud risk.</td>
</tr>
<tr>
<td>03</td>
<td>The transaction has been denied by the Gateway due to its high AVS risk.</td>
</tr>
<tr>
<td>04</td>
<td>The transaction has been denied by the Gateway due to an interchange timeout.</td>
</tr>
<tr>
<td>05</td>
<td>The transaction has been declined.</td>
</tr>
<tr>
<td>06</td>
<td>Transaction pending cardholder authentication.</td>
</tr>
<tr>
<td>07</td>
<td>The transaction was declined by the gateway and will not be processed due to retry optimization policy.</td>
</tr>
<tr>
<td>9</td>
<td>The transaction has been denied by the Gateway due to a LUHN check failure</td>
</tr>
<tr>
<td>10</td>
<td>The transaction has been partially approved.</td>
</tr>
<tr>
<td>11</td>
<td>The queried transaction is currently being processed. Please try again.</td>
</tr>
<tr>
<td>13</td>
<td>Rejected. The fraud-protection service is unavailable.</td>
</tr>
<tr>
<td>15</td>
<td>Rejected. Risk score is above limit.</td>
</tr>
</tbody>
</table>
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.

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

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>Partial match: Cardholder's Name does not match, but Street Address does. Returned only for the American Express card type.</td>
</tr>
<tr>
<td>U</td>
<td>Address information unavailable</td>
</tr>
<tr>
<td>V</td>
<td>Match: Cardholder's Name, Billing Address, and Billing Postal Code match. Returned only for the American Express card type.</td>
</tr>
<tr>
<td>W</td>
<td>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 match.</td>
</tr>
<tr>
<td>X</td>
<td>For US addresses: Full Match - Nine-digit ZIP Code and Address match</td>
</tr>
<tr>
<td>Y</td>
<td>Full Match - Five-digit ZIP Code and Address match</td>
</tr>
<tr>
<td>Z</td>
<td>Partial Match – Five-digit ZIP Code matches, but Address does not match</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Type</th>
<th>Full match</th>
<th>Partial match</th>
<th>No match</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. 5-digit ZIP Code</td>
<td>F, Y</td>
<td>A</td>
<td>N</td>
</tr>
<tr>
<td>International address</td>
<td>M</td>
<td>P</td>
<td>G</td>
</tr>
<tr>
<td>U.S. ZIP+4</td>
<td>X</td>
<td>W</td>
<td>N/A</td>
</tr>
<tr>
<td>No ZIP code</td>
<td>N/A</td>
<td>B</td>
<td>D</td>
</tr>
<tr>
<td>No address</td>
<td>N/A</td>
<td>Z</td>
<td>C</td>
</tr>
</tbody>
</table>
## 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 Source payment gateway. Your system should support receiving other values than the ones listed below.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Approved or completed successfully</td>
</tr>
<tr>
<td>01</td>
<td>Refer to card issuer</td>
</tr>
<tr>
<td>02</td>
<td>Refer to card issuer - special condition</td>
</tr>
<tr>
<td>03</td>
<td>Invalid merchant</td>
</tr>
<tr>
<td>04</td>
<td>Pick up card</td>
</tr>
<tr>
<td>05</td>
<td>Do not honour</td>
</tr>
<tr>
<td>06</td>
<td>Error</td>
</tr>
<tr>
<td>07</td>
<td>Pick up card - special condition</td>
</tr>
<tr>
<td>08</td>
<td>Honour with identification</td>
</tr>
<tr>
<td>10</td>
<td>Partial amount approved</td>
</tr>
<tr>
<td>12</td>
<td>Invalid transaction</td>
</tr>
<tr>
<td>13</td>
<td>Invalid amount</td>
</tr>
<tr>
<td>14</td>
<td>Invalid card number</td>
</tr>
<tr>
<td>15</td>
<td>No such issuer</td>
</tr>
<tr>
<td>19</td>
<td>Re-enter transaction</td>
</tr>
<tr>
<td>21</td>
<td>No action taken</td>
</tr>
<tr>
<td>30</td>
<td>Format error</td>
</tr>
<tr>
<td>34</td>
<td>Implausible card data</td>
</tr>
<tr>
<td>39</td>
<td>No credit account</td>
</tr>
<tr>
<td>41</td>
<td>Lost card, pick up</td>
</tr>
<tr>
<td>42</td>
<td>No universal account</td>
</tr>
<tr>
<td>43</td>
<td>Pick up, stolen card</td>
</tr>
<tr>
<td>44</td>
<td>No investment account</td>
</tr>
<tr>
<td>46</td>
<td>Closed account</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td>50</td>
<td>Do not renew</td>
</tr>
<tr>
<td>51</td>
<td>Insufficient funds</td>
</tr>
<tr>
<td>52</td>
<td>No checking account</td>
</tr>
<tr>
<td>53</td>
<td>No savings account</td>
</tr>
<tr>
<td>54</td>
<td>Expired card</td>
</tr>
<tr>
<td>55</td>
<td>Incorrect PIN</td>
</tr>
<tr>
<td>57</td>
<td>Transaction not allowed for cardholder</td>
</tr>
<tr>
<td>58</td>
<td>Transaction not permitted to terminal</td>
</tr>
<tr>
<td>59</td>
<td>Suspected fraud</td>
</tr>
<tr>
<td>61</td>
<td>Exceeds withdrawal limit</td>
</tr>
<tr>
<td>62</td>
<td>Restricted card</td>
</tr>
<tr>
<td>63</td>
<td>Security violation</td>
</tr>
<tr>
<td>64</td>
<td>Wrong original amount</td>
</tr>
<tr>
<td>65</td>
<td>Activity count limit exceeded</td>
</tr>
<tr>
<td>68</td>
<td>Response received too late</td>
</tr>
<tr>
<td>70</td>
<td>PIN data required</td>
</tr>
<tr>
<td>71</td>
<td>Decline, PIN not changed</td>
</tr>
<tr>
<td>75</td>
<td>PIN tries exceeded</td>
</tr>
<tr>
<td>76</td>
<td>Wrong PIN, number of PIN tries exceeded</td>
</tr>
<tr>
<td>77</td>
<td>Wrong Reference Number</td>
</tr>
<tr>
<td>78</td>
<td>Blocked, first used/ Record not found</td>
</tr>
<tr>
<td>79</td>
<td>Declined due to lifecycle event</td>
</tr>
<tr>
<td>80</td>
<td>Network error</td>
</tr>
<tr>
<td>81</td>
<td>PIN cryptographic error</td>
</tr>
<tr>
<td>82</td>
<td>Bad CVV/ Declined due to policy event</td>
</tr>
<tr>
<td>83</td>
<td>Transaction failed</td>
</tr>
<tr>
<td>84</td>
<td>Pre-authorization timed out</td>
</tr>
<tr>
<td>85</td>
<td>No reason to decline</td>
</tr>
<tr>
<td>86</td>
<td>Cannot verify PIN</td>
</tr>
<tr>
<td>87</td>
<td>Purchase amount only, no cashback allowed</td>
</tr>
<tr>
<td>88</td>
<td>Cryptographic failure</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>89</td>
<td>Authentication Failure</td>
</tr>
<tr>
<td>91</td>
<td>Issuer not available</td>
</tr>
<tr>
<td>92</td>
<td>Unable to route at acquirer module</td>
</tr>
<tr>
<td>93</td>
<td>Transaction cannot be completed, violation of law</td>
</tr>
<tr>
<td>94</td>
<td>Duplicate transmission</td>
</tr>
<tr>
<td>95</td>
<td>Reconcile error / Auth not found</td>
</tr>
<tr>
<td>96</td>
<td>System malfunction</td>
</tr>
<tr>
<td>97</td>
<td>Transaction has been declined by the processor</td>
</tr>
<tr>
<td>N3</td>
<td>Cash service not available</td>
</tr>
<tr>
<td>N4</td>
<td>Cash request exceeds issuer or approved limit</td>
</tr>
<tr>
<td>N7</td>
<td>CVV2 failure</td>
</tr>
<tr>
<td>R0</td>
<td>Stop Payment Order</td>
</tr>
<tr>
<td>R1</td>
<td>Revocation of Authorisation Order</td>
</tr>
<tr>
<td>R3</td>
<td>Revocation of all Authorisation Orders</td>
</tr>
<tr>
<td>1A</td>
<td>Strong Customer Authentication required</td>
</tr>
</tbody>
</table>
## Appendix E: z21 Possible Values

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d5</td>
<td>[a-zA-Z0-9=&quot;+]+</td>
<td>5</td>
<td>255</td>
<td>The browser’s user agent header</td>
</tr>
<tr>
<td>d6</td>
<td>[a-zA-Z]</td>
<td>2</td>
<td>16</td>
<td>Accept-Language header, comma-separated set of locales</td>
</tr>
<tr>
<td>d8</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Browser version</td>
</tr>
<tr>
<td>d9</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Device type (mobile, tablet, iPad, desktop, etc.)</td>
</tr>
<tr>
<td>d10</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Device Operating System name</td>
</tr>
<tr>
<td>d11</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Device Operating System version</td>
</tr>
</tbody>
</table>

### Retail

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

### Gaming

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ga1</td>
<td>[0-9]</td>
<td>1</td>
<td>16</td>
<td>Account Balance</td>
</tr>
<tr>
<td>ga2</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Game ID</td>
</tr>
<tr>
<td>ga3</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Game Name</td>
</tr>
</tbody>
</table>
### Source Payment Gateway API Specification

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ga4</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Time in Game (in seconds)</td>
</tr>
<tr>
<td>fo1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>9</td>
<td>Traded Currencies (XXX, YYY) Format</td>
</tr>
<tr>
<td>st1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Movie Name or Series Name</td>
</tr>
<tr>
<td>st2</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Movie or Series ID</td>
</tr>
</tbody>
</table>

### Forex

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fo1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>9</td>
<td>Traded currencies (XXX, YYY) format</td>
</tr>
</tbody>
</table>

### Streaming

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>st1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Movie name or series name</td>
</tr>
<tr>
<td>st2</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Movie or series ID</td>
</tr>
</tbody>
</table>

### Amount Components

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a41</td>
<td>[0-9]</td>
<td>1</td>
<td>12</td>
<td>Subtotal amount</td>
</tr>
<tr>
<td>a42</td>
<td>[0-9]</td>
<td>1</td>
<td>12</td>
<td>VAT amount</td>
</tr>
<tr>
<td>a44</td>
<td>[0-9]</td>
<td>1</td>
<td>12</td>
<td>Shipping amount</td>
</tr>
<tr>
<td>a46</td>
<td>[0-9]</td>
<td>1</td>
<td>12</td>
<td>Tip amount</td>
</tr>
</tbody>
</table>

### Furniture

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fu1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>50</td>
<td>The furniture supplier name</td>
</tr>
</tbody>
</table>
Car, Plane and Boat Rentals

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cr1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>50</td>
<td>The supplier/contractor name</td>
</tr>
</tbody>
</table>

Event Management

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ev1</td>
<td>YYYYMMDD</td>
<td>10</td>
<td>10</td>
<td>Event start date</td>
</tr>
<tr>
<td>ev2</td>
<td>YYYYMMDD</td>
<td>10</td>
<td>10</td>
<td>Event end date</td>
</tr>
<tr>
<td>ev3</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>50</td>
<td>Event organizer ID</td>
</tr>
<tr>
<td>ev4</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>50</td>
<td>Event ID</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ota1</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Ticket number</td>
</tr>
<tr>
<td>ota2</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Travel agency code</td>
</tr>
<tr>
<td>ota3</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Passenger name</td>
</tr>
<tr>
<td>ota5</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Travel agency</td>
</tr>
<tr>
<td>ota6</td>
<td>[a-zA-Z0-9]</td>
<td>3</td>
<td>128</td>
<td>E-ticket email address</td>
</tr>
<tr>
<td>ota7</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Airline name</td>
</tr>
<tr>
<td>ota12</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>64</td>
<td>Frequent Flier Number</td>
</tr>
<tr>
<td>ota14</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>1</td>
<td>Restricted Ticket Indicator. Indicates whether this ticket is non-refundable. Possible values: 0 - No restriction 1 - Restricted</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Min</td>
<td>Max</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>-------------</td>
</tr>
<tr>
<td>ota15</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>4</td>
<td>Computer Reservation System. Indicates the computerised reservation system used to make the reservation and purchase the ticket.</td>
</tr>
<tr>
<td>ota16</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>1</td>
<td>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</td>
</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>Name</td>
<td>Type</td>
<td>Min</td>
<td>Max</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-----</td>
<td>------</td>
<td>-------------</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 &quot;.&quot;:</td>
</tr>
<tr>
<td>fi2</td>
<td>[a-zA-Z0-9:]</td>
<td>9</td>
<td>48</td>
<td>Second flight information. Same format as fl1</td>
</tr>
<tr>
<td>fi3</td>
<td>[a-zA-Z0-9:]</td>
<td>9</td>
<td>48</td>
<td>Third flight information. Same format as fl1</td>
</tr>
<tr>
<td>fi4</td>
<td>[a-zA-Z0-9:]</td>
<td>9</td>
<td>48</td>
<td>Fourth flight information. Same format as fl1</td>
</tr>
<tr>
<td>fi5</td>
<td>YYYYMMDD</td>
<td>8</td>
<td>8</td>
<td>Flight departure date</td>
</tr>
<tr>
<td>fi6</td>
<td>YYYYMMDD</td>
<td>8</td>
<td>8</td>
<td>Flight arrival date</td>
</tr>
<tr>
<td>an1</td>
<td>[a-zA-Z0-9:]</td>
<td>8</td>
<td>38</td>
<td>First ancillary information. This field contains the following ancillary information delimited by &quot;.&quot;: (refer to Appendix K: Ancillary Fee Codes for more information).</td>
</tr>
<tr>
<td>an2</td>
<td>[a-zA-Z0-9:]</td>
<td>8</td>
<td>38</td>
<td>Second ancillary information. Same format as an1. Refer to Appendix K: Ancillary Fee Codes for more information.</td>
</tr>
</tbody>
</table>
### Source Payment Gateway API Specification

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>an3</td>
<td>[a-zA-Z0-9:]</td>
<td>8</td>
<td>38</td>
<td>Third ancillary information. Same format as an1. Refer to Appendix K: Ancillary Fee Codes for more information.</td>
</tr>
<tr>
<td>an4</td>
<td>[a-zA-Z0-9:]</td>
<td>8</td>
<td>38</td>
<td>Fourth ancillary information. Same format as an1. Refer to Appendix K: Ancillary Fee Codes for more information.</td>
</tr>
</tbody>
</table>

### Customer Identity

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c12</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>32</td>
<td>Customer Level (VIP, Basic)</td>
</tr>
<tr>
<td>c13</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>32</td>
<td>Customer ID (Shopper or Player ID)</td>
</tr>
<tr>
<td>c14</td>
<td>DATE</td>
<td>8</td>
<td>8</td>
<td>Customer Creation Date (YYYYMMDD)</td>
</tr>
<tr>
<td>c15</td>
<td>DATE</td>
<td>8</td>
<td>8</td>
<td>Customer Date of Birth (YYYYMMDD)</td>
</tr>
<tr>
<td>c16</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>32</td>
<td>Customer Username</td>
</tr>
<tr>
<td>c17</td>
<td>[a-zA-Z0-9]</td>
<td>3</td>
<td>255</td>
<td>Customer User Email</td>
</tr>
<tr>
<td>C18</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>32</td>
<td>ID / Passport number</td>
</tr>
</tbody>
</table>
## Appendix G: r1 Possible Values

A list of possible values for the r1 request parameter:

<table>
<thead>
<tr>
<th>#</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CREDORAX</td>
</tr>
<tr>
<td>2</td>
<td>Nuvei</td>
</tr>
<tr>
<td>3</td>
<td>ISRACARD</td>
</tr>
<tr>
<td>4</td>
<td>MAX</td>
</tr>
<tr>
<td>5</td>
<td>CAL</td>
</tr>
<tr>
<td>6</td>
<td>NBK</td>
</tr>
<tr>
<td>7</td>
<td>AMEX</td>
</tr>
<tr>
<td>8</td>
<td>Raiffeisen</td>
</tr>
<tr>
<td>9</td>
<td>BNP</td>
</tr>
<tr>
<td>10</td>
<td>Worldpay</td>
</tr>
</tbody>
</table>
Appendix H: Transaction Currencies

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

Note:
- Some processors may decline a transaction in a currency that was not authorised for your account.
- For currencies with two (2) exponents the two right most digits are considered the exponents (for example, if you want to process a transaction of GBP10.00 you should send the amount value as a4=1000)
- For currencies with three (3) exponents the three right most digits of the amount are considered the exponents. For example, to process a transaction of KWD10.000 you should send the amount value as a4=10000
- For currencies with zero exponents you should send the exact amount values. For example, JPY10 should be sent as a4=10

Notes:
1. Please refer to the Source Payment Gateway: Processors Specification to learn which currencies are supported by the processor.
2. For currencies with an exponent of 3, Visa requires the last digit to be 0. Transmitting the transactions in any other format may cause the transaction to be declined.

<table>
<thead>
<tr>
<th>Country</th>
<th>Currency</th>
<th>Currency Code</th>
<th>Exponent</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Arab Emirates</td>
<td>United Arab Emirates Dirham</td>
<td>AED</td>
<td>2</td>
</tr>
<tr>
<td>Afghanistan</td>
<td>Afghani</td>
<td>AFN</td>
<td>2</td>
</tr>
<tr>
<td>Albania</td>
<td>Lek</td>
<td>ALL</td>
<td>2</td>
</tr>
<tr>
<td>Armenia</td>
<td>Armenian Dram</td>
<td>AMD</td>
<td>2</td>
</tr>
<tr>
<td>Netherlands Antilles</td>
<td>Netherlands Antillean Guilder</td>
<td>ANG</td>
<td>2</td>
</tr>
<tr>
<td>Angola</td>
<td>Kwanza</td>
<td>AOA</td>
<td>2</td>
</tr>
<tr>
<td>Argentina</td>
<td>Argentine Peso</td>
<td>ARS</td>
<td>2</td>
</tr>
<tr>
<td>Australia</td>
<td>Australian Dollar</td>
<td>AUD</td>
<td>2</td>
</tr>
<tr>
<td>Country</td>
<td>Currency</td>
<td>Currency Code</td>
<td>Exponent</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>Aruba</td>
<td>Aruban Guilder</td>
<td>AWG</td>
<td>2</td>
</tr>
<tr>
<td>Azerbaijan</td>
<td>Azerbaijani Manat</td>
<td>AZN</td>
<td>2</td>
</tr>
<tr>
<td>Bosnia Herzegovina</td>
<td>Convertible Marks</td>
<td>BAM</td>
<td>2</td>
</tr>
<tr>
<td>Barbados</td>
<td>Barbados Dollar</td>
<td>BBD</td>
<td>2</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Bangladeshi Taka</td>
<td>BDT</td>
<td>2</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>Bulgarian Lev</td>
<td>BGN</td>
<td>2</td>
</tr>
<tr>
<td>Bahrain</td>
<td>Bahraini Dinar</td>
<td>BHD</td>
<td>3</td>
</tr>
<tr>
<td>Burundi</td>
<td>Burundian Franc</td>
<td>BIF</td>
<td>0</td>
</tr>
<tr>
<td>Bermuda</td>
<td>Bermuda</td>
<td>BMD</td>
<td>2</td>
</tr>
<tr>
<td>Brunei Darussalam</td>
<td>Brunei Dollar</td>
<td>BND</td>
<td>2</td>
</tr>
<tr>
<td>Bolivia</td>
<td>Boliviano</td>
<td>BOB</td>
<td>2</td>
</tr>
<tr>
<td>Brazil</td>
<td>Brazilian Real</td>
<td>BRL</td>
<td>2</td>
</tr>
<tr>
<td>Bahamas</td>
<td>Bahamian Dollar</td>
<td>BSD</td>
<td>2</td>
</tr>
<tr>
<td>Bhutan</td>
<td>Ngultrum</td>
<td>BTN</td>
<td>2</td>
</tr>
<tr>
<td>Botswana</td>
<td>Pula</td>
<td>BWP</td>
<td>2</td>
</tr>
<tr>
<td>Belarus</td>
<td>New Belarussian Ruble</td>
<td>BYN</td>
<td>2</td>
</tr>
<tr>
<td>Belize</td>
<td>Belize Dollar</td>
<td>BZD</td>
<td>2</td>
</tr>
<tr>
<td>Canada</td>
<td>Canadian Dollar</td>
<td>CAD</td>
<td>2</td>
</tr>
<tr>
<td>Congo, The Democratic Republic of</td>
<td>Franc Congolais</td>
<td>CDF</td>
<td>2</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Swiss Franc</td>
<td>CHF</td>
<td>2</td>
</tr>
<tr>
<td>Chile</td>
<td>Chilean Peso</td>
<td>CLP</td>
<td>0</td>
</tr>
<tr>
<td>China</td>
<td>Chinese Yuan</td>
<td>CNY</td>
<td>2</td>
</tr>
<tr>
<td>Colombia</td>
<td>Colombian Peso</td>
<td>COP</td>
<td>2</td>
</tr>
<tr>
<td>Costa Rica</td>
<td>Costa Rican Colon</td>
<td>CRC</td>
<td>2</td>
</tr>
<tr>
<td>Cape Verde</td>
<td>Cape Verde Escudo</td>
<td>CVE</td>
<td>2</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Czech Koruna</td>
<td>CZK</td>
<td>2</td>
</tr>
<tr>
<td>Djibouti</td>
<td>Djibouti Franc</td>
<td>DJF</td>
<td>0</td>
</tr>
<tr>
<td>Denmark</td>
<td>Danish Krone</td>
<td>DKK</td>
<td>2</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>Dominican Peso</td>
<td>DOP</td>
<td>2</td>
</tr>
<tr>
<td>Algeria</td>
<td>Algerian Dinar</td>
<td>DZD</td>
<td>2</td>
</tr>
<tr>
<td>Country</td>
<td>Currency</td>
<td>Currency Code</td>
<td>Exponent</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>Estonia</td>
<td>Kroon</td>
<td>EEK</td>
<td>2</td>
</tr>
<tr>
<td>Egypt</td>
<td>Egyptian Pound</td>
<td>EGP</td>
<td>2</td>
</tr>
<tr>
<td>Eritrea</td>
<td>Nakfa</td>
<td>ERN</td>
<td>2</td>
</tr>
<tr>
<td>Ethiopia</td>
<td>Ethiopian Birr</td>
<td>ETB</td>
<td>2</td>
</tr>
<tr>
<td><strong>19 European Union</strong></td>
<td><strong>Countries (EMU)</strong></td>
<td><strong>EUR</strong></td>
<td><strong>2</strong></td>
</tr>
<tr>
<td>Fiji</td>
<td>Fiji Dollar</td>
<td>FJD</td>
<td>2</td>
</tr>
<tr>
<td>Falkland Islands (Malvinas)</td>
<td>Falkland Islands Pound</td>
<td>FKP</td>
<td>2</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Pounds Sterling</td>
<td>GBP</td>
<td>2</td>
</tr>
<tr>
<td>Georgia</td>
<td>Lari</td>
<td>GEL</td>
<td>2</td>
</tr>
<tr>
<td>Ghana</td>
<td>Cedi</td>
<td>GHS</td>
<td>2</td>
</tr>
<tr>
<td>Gibraltar</td>
<td>Gibraltar Pound</td>
<td>GIP</td>
<td>2</td>
</tr>
<tr>
<td>Gambia</td>
<td>Dalasi</td>
<td>GMD</td>
<td>2</td>
</tr>
<tr>
<td>Guinea</td>
<td>Guinea Franc</td>
<td>GNF</td>
<td>0</td>
</tr>
<tr>
<td>Guatemala</td>
<td>Quetzal</td>
<td>GTQ</td>
<td>2</td>
</tr>
<tr>
<td>Guyana</td>
<td>Guyana Dollar</td>
<td>GYD</td>
<td>2</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>Hong Kong Dollars</td>
<td>HKD</td>
<td>2</td>
</tr>
<tr>
<td>Honduras</td>
<td>Lempira</td>
<td>HNL</td>
<td>2</td>
</tr>
<tr>
<td>Croatia</td>
<td>Croatian Kuna</td>
<td>HRK</td>
<td>2</td>
</tr>
<tr>
<td>Haiti</td>
<td>Haitian Gourde</td>
<td>HTG</td>
<td>2</td>
</tr>
<tr>
<td>Hungary</td>
<td>Forint</td>
<td>HUF</td>
<td>2</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Rupiah</td>
<td>IDR</td>
<td>2</td>
</tr>
<tr>
<td>Israel</td>
<td>Israeli New Sheqel</td>
<td>ILS</td>
<td>2</td>
</tr>
<tr>
<td>India</td>
<td>Indian Rupee</td>
<td>INR</td>
<td>2</td>
</tr>
<tr>
<td>Iraq</td>
<td>Iraqi Dinar</td>
<td>IQD</td>
<td>3</td>
</tr>
<tr>
<td>Iceland</td>
<td>Iceland Krona</td>
<td>ISK</td>
<td>0</td>
</tr>
<tr>
<td>Jamaica</td>
<td>Jamaican Dollar</td>
<td>JMD</td>
<td>2</td>
</tr>
<tr>
<td>Jordan</td>
<td>Jordanian Dinar</td>
<td>JOD</td>
<td>3</td>
</tr>
<tr>
<td>Japan</td>
<td>Japanese Yen</td>
<td>JPY</td>
<td>0</td>
</tr>
<tr>
<td>Kenya</td>
<td>Kenyan Shilling</td>
<td>KES</td>
<td>2</td>
</tr>
<tr>
<td>Kyrgyzstan</td>
<td>Som</td>
<td>KGS</td>
<td>2</td>
</tr>
<tr>
<td>Country</td>
<td>Currency</td>
<td>Currency Code</td>
<td>Exponent</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cambodia</td>
<td>Riel</td>
<td>KHR</td>
<td>2</td>
</tr>
<tr>
<td>Comoros</td>
<td>Comoro Franc</td>
<td>KMF</td>
<td>0</td>
</tr>
<tr>
<td>Korea, Republic of</td>
<td>South Korean Won</td>
<td>KRW</td>
<td>0</td>
</tr>
<tr>
<td>Kuwait</td>
<td>Kuwaiti Dinar</td>
<td>KWD</td>
<td>3</td>
</tr>
<tr>
<td>Cayman Islands</td>
<td>Cayman Islands Dollar</td>
<td>KYD</td>
<td>2</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>Tenge</td>
<td>KZT</td>
<td>2</td>
</tr>
<tr>
<td>Lao People's Democratic Republic</td>
<td>Kip</td>
<td>LAK</td>
<td>2</td>
</tr>
<tr>
<td>Lebanon</td>
<td>Lebanese Pound</td>
<td>LBP</td>
<td>2</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>Sri Lanka Rupee</td>
<td>LKR</td>
<td>2</td>
</tr>
<tr>
<td>Liberia</td>
<td>Liberian Dollar</td>
<td>LRD</td>
<td>2</td>
</tr>
<tr>
<td>Lesotho</td>
<td>Lesotho Loti</td>
<td>LSL</td>
<td>2</td>
</tr>
<tr>
<td>Lithuania</td>
<td>Lithuanian Litas</td>
<td>LTL</td>
<td>2</td>
</tr>
<tr>
<td>Libyan Arab Jamahiriya</td>
<td>Libyan Dinar</td>
<td>LYD</td>
<td>3</td>
</tr>
<tr>
<td>Morocco</td>
<td>Moroccan Dirham</td>
<td>MAD</td>
<td>2</td>
</tr>
<tr>
<td>Moldova, Republic of</td>
<td>Moldovan Leu</td>
<td>MDL</td>
<td>2</td>
</tr>
<tr>
<td>Madagascar</td>
<td>Malagasy Ariary</td>
<td>MGA</td>
<td>2</td>
</tr>
<tr>
<td>Macedonia</td>
<td>Denar</td>
<td>MKD</td>
<td>2</td>
</tr>
<tr>
<td>Myanmar</td>
<td>Kyat</td>
<td>MMK</td>
<td>2</td>
</tr>
<tr>
<td>Mongolia</td>
<td>Tugrik</td>
<td>MNT</td>
<td>2</td>
</tr>
<tr>
<td>Macao</td>
<td>Pataca</td>
<td>MOP</td>
<td>2</td>
</tr>
<tr>
<td>Mauritania</td>
<td>Ouguiya</td>
<td>MRO</td>
<td>2</td>
</tr>
<tr>
<td>Mauritania</td>
<td>Mauritania</td>
<td>MRU</td>
<td>2</td>
</tr>
<tr>
<td>Mauritius</td>
<td>Mauritius Rupee</td>
<td>MUR</td>
<td>2</td>
</tr>
<tr>
<td>Maldives</td>
<td>Rufiyaa</td>
<td>MVR</td>
<td>2</td>
</tr>
<tr>
<td>Malawi</td>
<td>Kwacha</td>
<td>MWK</td>
<td>2</td>
</tr>
<tr>
<td>Mexico</td>
<td>Mexican Peso</td>
<td>MXN</td>
<td>2</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Malaysian Ringgit</td>
<td>MYR</td>
<td>2</td>
</tr>
<tr>
<td>Mozambique</td>
<td>Metical</td>
<td>MZN</td>
<td>2</td>
</tr>
<tr>
<td>Namibia</td>
<td>Namibian Dollar</td>
<td>NAD</td>
<td>2</td>
</tr>
<tr>
<td>Nigeria</td>
<td>Naira</td>
<td>NGN</td>
<td>2</td>
</tr>
<tr>
<td>Country</td>
<td>Currency</td>
<td>Currency Code</td>
<td>Exponent</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>Nicaragua</td>
<td>Cordoba Oro</td>
<td>NIO</td>
<td>2</td>
</tr>
<tr>
<td>Norway</td>
<td>Norwegian Krone</td>
<td>NOK</td>
<td>2</td>
</tr>
<tr>
<td>Nepal</td>
<td>Nepalese Rupee</td>
<td>NPR</td>
<td>2</td>
</tr>
<tr>
<td>New Zealand</td>
<td>New Zealand Dollar</td>
<td>NZD</td>
<td>2</td>
</tr>
<tr>
<td>Oman</td>
<td>Omani Rial</td>
<td>OMR</td>
<td>3</td>
</tr>
<tr>
<td>Panama</td>
<td>Balboa</td>
<td>PAB</td>
<td>2</td>
</tr>
<tr>
<td>Peru</td>
<td>Nuevo Sol</td>
<td>PEN</td>
<td>2</td>
</tr>
<tr>
<td>Independent State of Papua New Guinea</td>
<td>Kina</td>
<td>PGK</td>
<td>2</td>
</tr>
<tr>
<td>Philippines</td>
<td>Philippine Peso</td>
<td>PHP</td>
<td>2</td>
</tr>
<tr>
<td>Pakistan</td>
<td>Pakistani Rupee</td>
<td>PKR</td>
<td>2</td>
</tr>
<tr>
<td>Poland</td>
<td>Zloty</td>
<td>PLN</td>
<td>2</td>
</tr>
<tr>
<td>Paraguay</td>
<td>Guarani</td>
<td>PYG</td>
<td>0</td>
</tr>
<tr>
<td>Qatar</td>
<td>Qatari Rial</td>
<td>QAR</td>
<td>2</td>
</tr>
<tr>
<td>Romania</td>
<td>Romanian New Leu</td>
<td>RON</td>
<td>2</td>
</tr>
<tr>
<td>Serbia</td>
<td>Serbian Dinar</td>
<td>RSD</td>
<td>2</td>
</tr>
<tr>
<td>Russia</td>
<td>Russian Rouble</td>
<td>RUB</td>
<td>2</td>
</tr>
<tr>
<td>Rwanda</td>
<td>Rwanda Franc</td>
<td>RWF</td>
<td>0</td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>Saudi Riyal</td>
<td>SAR</td>
<td>2</td>
</tr>
<tr>
<td>Solomon Islands</td>
<td>Solomon Islands Dollar</td>
<td>SBD</td>
<td>2</td>
</tr>
<tr>
<td>Seychelles</td>
<td>Seychelles Rupees</td>
<td>SCR</td>
<td>2</td>
</tr>
<tr>
<td>Sweden</td>
<td>Swedish Krona/Kronor</td>
<td>SEK</td>
<td>2</td>
</tr>
<tr>
<td>Singapore</td>
<td>Singapore Dollar</td>
<td>SGD</td>
<td>2</td>
</tr>
<tr>
<td>Saint Helena, Ascension and Tristan Da Cunha</td>
<td>Saint Helena Pound</td>
<td>SHP</td>
<td>2</td>
</tr>
<tr>
<td>Sierra Leone</td>
<td>Leone</td>
<td>SLL</td>
<td>2</td>
</tr>
<tr>
<td>Somalia, Federal Republic of</td>
<td>Somali Shilling</td>
<td>SOS</td>
<td>2</td>
</tr>
<tr>
<td>Suriname</td>
<td>Surinam Dollar</td>
<td>SRD</td>
<td>2</td>
</tr>
<tr>
<td>South Sudan</td>
<td>South Sudanese Pound</td>
<td>SSP</td>
<td>2</td>
</tr>
<tr>
<td>Sao Tome and Principe</td>
<td>Dobra</td>
<td>STD</td>
<td>2</td>
</tr>
<tr>
<td>Sao Tome and Principe</td>
<td>Sao Tome Principe</td>
<td>STN</td>
<td>2</td>
</tr>
<tr>
<td>Country</td>
<td>Currency</td>
<td>Currency Code</td>
<td>Exponent</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>El Salvador</td>
<td>El Salvador Colon</td>
<td>SVC</td>
<td>2</td>
</tr>
<tr>
<td>Syrian Arab Republic</td>
<td>Syrian Pound</td>
<td>SYP</td>
<td>2</td>
</tr>
<tr>
<td>Swaziland</td>
<td>Lilangeni</td>
<td>SZL</td>
<td>2</td>
</tr>
<tr>
<td>Thailand</td>
<td>Baht</td>
<td>THB</td>
<td>2</td>
</tr>
<tr>
<td>Tajikistan</td>
<td>Somoni</td>
<td>TJS</td>
<td>2</td>
</tr>
<tr>
<td>Turkmenistan</td>
<td>Manat</td>
<td>TMT</td>
<td>2</td>
</tr>
<tr>
<td>Tunisia</td>
<td>Tunisian Dinar</td>
<td>TND</td>
<td>3</td>
</tr>
<tr>
<td>Tonga</td>
<td>Paanga</td>
<td>TOP</td>
<td>2</td>
</tr>
<tr>
<td>Turkey</td>
<td>Turkish Lira</td>
<td>TRY</td>
<td>2</td>
</tr>
<tr>
<td>Trinidad And Tobago</td>
<td>Trinidad and Tobago Dollar</td>
<td>TTD</td>
<td>2</td>
</tr>
<tr>
<td>Taiwan Province of China</td>
<td>New Taiwan Dollar</td>
<td>TWD</td>
<td>2</td>
</tr>
<tr>
<td>Tanzania, United Republic of</td>
<td>Tanzanian Shilling</td>
<td>TZS</td>
<td>2</td>
</tr>
<tr>
<td>Ukraine</td>
<td>Hryvnia</td>
<td>UAH</td>
<td>2</td>
</tr>
<tr>
<td>Uganda</td>
<td>Uganda Shilling</td>
<td>UGX</td>
<td>2</td>
</tr>
<tr>
<td>United States</td>
<td>US Dollar</td>
<td>USD</td>
<td>2</td>
</tr>
<tr>
<td>Uruguay</td>
<td>Peso Uruguayo</td>
<td>UYU</td>
<td>2</td>
</tr>
<tr>
<td>Uzbekistan</td>
<td>Uzbekistan Som</td>
<td>UZS</td>
<td>2</td>
</tr>
<tr>
<td>Venezuela</td>
<td>Venezuelan Bolivar Fuerte</td>
<td>VEF</td>
<td>2</td>
</tr>
<tr>
<td>Vietnam</td>
<td>Vietnamese Đồng</td>
<td>VND</td>
<td>0</td>
</tr>
<tr>
<td>Vanuatu</td>
<td>Vatu</td>
<td>VUV</td>
<td>0</td>
</tr>
<tr>
<td>Samoa</td>
<td>Samoan Tala</td>
<td>WST</td>
<td>2</td>
</tr>
<tr>
<td>Central African Republic</td>
<td>CFA Franc BEAC</td>
<td>XAF</td>
<td>0</td>
</tr>
<tr>
<td>Eastern Caribbean States</td>
<td>East Caribbean Dollar</td>
<td>XCD</td>
<td>2</td>
</tr>
<tr>
<td>Communauté Financière Africaine</td>
<td>CFA Franc BCEAO</td>
<td>XOF</td>
<td>0</td>
</tr>
<tr>
<td>French Polynesia</td>
<td>CFP Franc</td>
<td>XPF</td>
<td>0</td>
</tr>
<tr>
<td>Yemen</td>
<td>Yemeni Rial</td>
<td>YER</td>
<td>2</td>
</tr>
<tr>
<td>South Africa</td>
<td>South African Rand</td>
<td>ZAR</td>
<td>2</td>
</tr>
<tr>
<td>Zambia</td>
<td>Kwacha</td>
<td>ZMW</td>
<td>2</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>Fourth Zimbabwe Dollar</td>
<td>ZWL</td>
<td>2</td>
</tr>
<tr>
<td>Zimbabwe</td>
<td>Third Zimbabwe Dollar</td>
<td>ZWR</td>
<td>2</td>
</tr>
</tbody>
</table>
Appendix I: SCA & 3D Secure

This section describes the specifications for using the Source Payment Gateway 3D Secure service. If you are using a third-party 3D Secure service, prior to sending the transaction to Source 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.

Source Payment Gateway offers two modules of 3D Secure:

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

**NOTE:**

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

Contact your account manager for more information!

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

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

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

### 3D Secure Transaction Flow

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

**Note:**
- The 3D Secure transaction flow may require more steps in order to complete the transaction
- For the challenge flow consider implementation of a notification mechanism to automatically retrieve updates on the transaction processing progress without initiating another call to the gateway. Contact your account manager for more details on how to enrol 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:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Initiate 3D Secure before completing the payment</td>
</tr>
<tr>
<td>02</td>
<td>Process payment without 3D Secure</td>
</tr>
<tr>
<td>03</td>
<td>Initiate 3D Secure according to the 3DS Adviser result (see 3DS Adviser)</td>
</tr>
<tr>
<td>04</td>
<td>Only initiate the 3DS Adviser service. Relevant only for op code 98</td>
</tr>
</tbody>
</table>

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

Standard 3D Secure Workflow

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

A. No challenge (frictionless experience)
B. Device fingerprint assessment only (frictionless experience)
C. Cardholder challenge only (without device fingerprint)
D. Full authentication (both device fingerprint assessment and cardholder challenge)

The entities participating in the 3D secure process are:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>The cardholder's browser from which the process was initiated</td>
</tr>
<tr>
<td>Merchant Server</td>
<td>The merchant’s server side</td>
</tr>
<tr>
<td>Source</td>
<td>Source Payment Gateway</td>
</tr>
<tr>
<td>Issuer</td>
<td>The issuer of the card used in the transaction</td>
</tr>
</tbody>
</table>
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 Source Payment Gateway.

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

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

Step 6 – Source sends the transaction response with the result of the payment and the 3D secure process.
Source Payment Gateway API Specification

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 Source Payment Gateway.

Steps 3-5: Source 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: Source 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: Source initiates the payment.

Step 11: Source 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 Source Payment Gateway
Steps 3-4: Source Payment Gateway initiates the 3D secure authentication process. Cardholder authentication is needed.
Step 5: Source 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: Source receives the authentication results from the Issuer.
Step 10: Credorax initiates the payment
Step 11: Source sends notification to the merchant with all payment & authentication results.
Step 12: Source 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 Source Payment Gateway.
Step 3-5: Source 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: Source 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: Source 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: Source receives the authentication results from the Issuer.
Step 14: Source Payment Gateway initiates the payment
Step 15: Source sends notification to the merchant with all payment & authentication results.
Step 16: Source redirects the browser to the merchant site.
Device fingerprint information retrieval flow

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_method</td>
<td>URL</td>
<td>The issuer’s URL that should be used to trigger the collection of the device fingerprint by the issuer</td>
</tr>
<tr>
<td>3ds_trxid</td>
<td>[a-zA-Z0-9,-]</td>
<td>Universally unique transaction identifier to identify a single 3DS transaction.</td>
</tr>
</tbody>
</table>

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 Source.

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.

   **Take 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 Credorax. This is done by sending operation code [92] in the following structure:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Length</th>
<th>Completion Operation [92]</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>Source assigned gateway Merchant ID</td>
<td>[A-Z0-9_]</td>
<td>3,6</td>
<td>m</td>
</tr>
<tr>
<td>K</td>
<td>Unique cipher used for authenticating requests</td>
<td>[0-9A-Za-z]</td>
<td>1,32</td>
<td>m</td>
</tr>
<tr>
<td>O</td>
<td>Operation Code</td>
<td>The operation code is used to determine the requested service.</td>
<td>[0-9]</td>
<td>1,3</td>
</tr>
<tr>
<td>a1</td>
<td>Request ID</td>
<td>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.</td>
<td>[A-Za-z0-9-]</td>
<td>1,32</td>
</tr>
<tr>
<td>g5</td>
<td>Referred transaction ID. Populate this field with the received z1 of the original transaction.</td>
<td>[0-9]</td>
<td>m</td>
<td></td>
</tr>
<tr>
<td>3ds_trxid</td>
<td>Universally unique transaction identifier to identify a single 3DS transaction.</td>
<td>[a-zA-Z0-9, -]</td>
<td>36,36</td>
<td>m</td>
</tr>
<tr>
<td>3ds_compind</td>
<td>Received from the issuer. Indicates whether the device fingerprint collection completed successfully.</td>
<td>[Y, N]</td>
<td>1,1</td>
<td>m</td>
</tr>
</tbody>
</table>

**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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Min</th>
<th>Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>f23</td>
<td>[0-9]</td>
<td>1</td>
<td>3</td>
<td>Assigns an ad-hoc threshold that extends the regular fraud threshold, for authorised 3D secure transactions only.</td>
</tr>
</tbody>
</table>

Additional Response parameters for the 3DS Adviser Module

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>o/m</th>
<th>Min, Max</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exemption_action</td>
<td>[0-9]</td>
<td>o</td>
<td>2,2</td>
<td>Indicates the merchant preference regarding SCA exemption. Possible values are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>01: Do not request exemption. This is the default behavior for the Credorax Gateway. If the field is absent from the transaction request, no exemption will be applied.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>02: Request an exemption as part of the payment request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>03: Request an exemption as part of the 3D Secure request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>04: Request exemption by default. Credorax will apply for exemption as part of the 3D Secure request if possible.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note: If no value is provided, and you are using the 3DS Adviser module, the Credorax Payment Gateway requests an exemption (if applicable) as part of the 3D secure process.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>o/m</td>
<td>Min, Max</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>------</td>
<td>-----</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exemption_reason</td>
<td>[0-9]</td>
<td>o</td>
<td>2.2</td>
<td>This field is required when exemption_action = 02 or 03. Possible values: 01: Low value transaction (below 30 EUR or equivalent) 02: Low risk transaction (TRA) (^1) 03: Request Trusted Beneficiary Indicator (Whitelisting) (^2) 04: Secure Corporate Cards (^3) 05: Delegated Authentication (^4) 06: MIT – Recurring same amount 07: MIT – other (^5) 08: Trusted Beneficiary Indicator (Whitelisting) – Done (^6) (^1) Requires real-time fraud monitoring solutions (^2) Use this value to indicate to the ACS to obtain confirmation from the cardholder to whitelist the merchant for future purchases (^3) This is not a standard exemption you can request. If you know the card used for the transaction is a secure corporate card, use this value to indicate so to Credorax. 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 Credorax gateway that this is a potential whitelisting card. This will help the 3DS Adviser determine the optimal 3D Secure employment.</td>
</tr>
<tr>
<td>tra_score</td>
<td>[0-9,A-Za-z]</td>
<td>c</td>
<td>1.8</td>
<td>Indicates the transaction risk analysis result calculated by a third party provider as a basis for exemption_reason=02</td>
</tr>
</tbody>
</table>
Managing SCA for Merchant initiated transaction

Merchant initiated transactions can occur in two business cases:

1. Recurring transaction, where the first original transaction was initiated by the cardholder (for example, initiating a subscription to a product or service). In this case the initial transaction is subject to SCA, but any subsequent transaction can be exempted from SCA.

2. Periodic charges, always initiated by the merchant, based on card details provided by the cardholder not as part of a specific transaction (for example, the cardholder provided their card details to pay utility bills). In this case all subsequent payments will be out of scope except for the initial transaction which is subjected to SCA. In order to properly identify merchant-initiated transactions we added two new parameters you should be prepared to send and receive.

Note: for recurring transactions where the first transaction occurred before 14 September 2019, use the static value = 999999999999999. This ensures the transaction will be processed without an additional request for SCA.

Exemption – Response Parameters

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

3D Secure Authentication-Only Flow

You may choose to use the Source Payment Gateway 3D Secure Service without completing the transaction processing through the Source 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:

<table>
<thead>
<tr>
<th>Requested Data</th>
<th>Credorax Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser IP address</td>
<td>d1</td>
<td>IP address of the browser as returned by the HTTP headers. In either ipv4 or ipv6 format</td>
</tr>
<tr>
<td>Buyer email address</td>
<td>c3</td>
<td>Cardholder's email address in valid email address format, such as <a href="mailto:joe@bloggs.com">joe@bloggs.com</a></td>
</tr>
<tr>
<td>Billing Information</td>
<td>c4</td>
<td>Cardholder Billing Address street number</td>
</tr>
<tr>
<td></td>
<td>c5</td>
<td>Cardholder Billing Address street name</td>
</tr>
<tr>
<td></td>
<td>c7</td>
<td>Cardholder Billing Address city name</td>
</tr>
<tr>
<td></td>
<td>c8</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>c9</td>
<td>Cardholder Billing Address Country Code. Please refer to ISO 3166-1-alpha-2 for a list</td>
</tr>
<tr>
<td></td>
<td>c10</td>
<td>Cardholder Billing Address Postal/ZIP Code</td>
</tr>
<tr>
<td>Shipping information</td>
<td>3ds_shipaddrcity</td>
<td>City of the shipping address requested by the Cardholder</td>
</tr>
<tr>
<td></td>
<td>3ds_shipaddrcountry</td>
<td>Country of the shipping address requested by the Cardholder. Please refer to ISO 3166-1-alpha-2 for a list</td>
</tr>
<tr>
<td></td>
<td>3ds_shipaddrline1</td>
<td>First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase</td>
</tr>
</tbody>
</table>
## Requested Data

<table>
<thead>
<tr>
<th>Credorax Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_shipaddrline2</td>
<td>Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase</td>
</tr>
<tr>
<td>3ds_shipaddrpostcode</td>
<td>ZIP or other postal code of the shipping address associated with the card used for this purchase</td>
</tr>
<tr>
<td>3ds_shipaddrstate</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Do Shipping and Billing addresses match?

- **3ds_addrmatch**: Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical.

## Request parameters

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>min</th>
<th>max</th>
<th>m/o/c</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_channel</td>
<td>Indicates the type of channel interface being used to initiate the transaction. The accepted values are:</td>
<td>[0-3]</td>
<td>2</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>01 - App-based (APP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - Browser (BRW)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 - 3DS Requestor Initiated (3RI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_redirect_url</td>
<td>Contains the merchant URL to which the browser should be redirected after the challenge session</td>
<td>[a-zA-Z0-9]</td>
<td>0</td>
<td>2048</td>
<td>m</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_category</td>
<td>Identifies the category of the message for a specific use case. The accepted values are:</td>
<td>[0-3]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>01 - PA (Payment authentication)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - NPA (NON-payment authentication)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>80 - Data only (Mastercard only, valid only for 3ds_channel = 01 or 02)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_compind</td>
<td>Relevant only if 3ds_channel = 02.</td>
<td>[Y,N,U]</td>
<td>1</td>
<td>1</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>Received as part of the op code 92 flow.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>m when 3ds_channel=02</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_sdkinterface</td>
<td>Specifies the SDK Interface types that the device supports for displaying specific challenge user interfaces within the SDK. Accepted values are:</td>
<td>[0-3]</td>
<td>2</td>
<td>2</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>01 - Native</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - HTML</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 - Both</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_sdkuitype</td>
<td>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:</td>
<td>Comma</td>
<td>2</td>
<td>14</td>
<td>c</td>
</tr>
<tr>
<td></td>
<td>01 - Text</td>
<td>separat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - Single select</td>
<td>ed list</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 - Multi select</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04 - OOB</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>05 - Html Other (valid only for HTML UI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>For Native UI SDK Interface accepted values are 01-04 and for HTML UI accepted values are 01-05.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_reqauthmethod</td>
<td>Information about how the cardholder was authenticated before or during the</td>
<td>[0-6]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>transaction. The mechanism used by the Cardholder to authenticate to the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>merchant. Accepted values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 01 - No authentication occurred (i.e., cardholder &quot;logged in&quot; as guest)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 02 - Login to the cardholder account at the merchant system using merchant's</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>own credentials</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 03 - Login to the cardholder account at the merchant system using federated ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 04 - Login to the cardholder account at the merchant system using issuer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>credentials</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 05 - Login to the cardholder account at the merchant system using third-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>party authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 06 - Login to the cardholder account at the merchant system using FIDO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authenticator</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 07 - Login to the cardholder account at the merchant system using FIDO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Authenticator (applicable for 3DS version 2.2 and above)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 08 - SRC Assurance Data. (applicable for 3DS version 2.2 and above)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_reqauthtimestamp</td>
<td>Date and time in UTC of the cardholder authentication. Field is limited to</td>
<td>[0-9]</td>
<td>12</td>
<td>12</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>12 characters and the accepted format is YYYYMMDDHHMM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_reqauthdata</td>
<td>Data that documents and supports a specific authentication process. The intention is that for each</td>
<td>[a-zA-Z0-9]</td>
<td>0</td>
<td>255</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>merchant Authentication Method, this field contains data that the issuer can use to verify the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>authentication process.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_reqchallengeid</td>
<td>Indicates whether a challenge is requested for this transaction. For example: For 3ds_category 01-PA,</td>
<td>[0-4]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>a merchant may have concerns about the transaction, and request a challenge. For 3ds_category</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02-NPA, a challenge may be necessary when adding a new card to a wallet.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 - No preference</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - No challenge requested</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 - Challenge requested by merchant</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04 - Challenge requested: Mandate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>05 - No Challenge Requested, transactional risk analysis is already performed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>06 - No Challenge Requested, Data share only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>07 - No Challenge Requested, SCA is already performed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>08 - No challenge requested (utilise whitelist exemption if no challenge required)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>09 - Challenge requested (whitelist prompt requested if challenge required)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_reqpriorref</td>
<td>This data element provides additional information to the issuer to determine the best approach for</td>
<td>[a-zA-Z0-9]</td>
<td>36</td>
<td>36</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>handling a request. The element contains the issuer’s Transaction ID for a prior authenticated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>transaction (for example, the first recurring transaction that was authenticated with the</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>cardholder).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_reqpriorauthmethod</td>
<td>Mechanism used by the Cardholder to previously authenticate to the merchant.</td>
<td>[0-4]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Accepted values for this field are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 - Frictionless authentication occurred by issuer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - Cardholder challenge occurred by issuer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 - AVS verified</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04 - Other issuer methods</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_reqpriorauthtimestamp</td>
<td>Date and time in UTC of the prior authentication. Accepted date format is YYYYMMDDHHMM.</td>
<td>[0-9]</td>
<td>12</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>3ds_reqpriorauthdata</td>
<td>Data that documents and supports a specific authentication process. In the current version of the specification this data element is not defined in detail, however the intention is that for each merchant Authentication Method, this field carry data that the issuer can use to verify the authentication process. In future versions of the application, these details are expected to be included. Field is limited to a maximum of 2048 characters.</td>
<td>[a-zA-Z0-9]</td>
<td>0</td>
<td>255</td>
<td>o</td>
</tr>
<tr>
<td>3ds_reqdecreqind</td>
<td>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:</td>
<td>[Y,N]</td>
<td>1</td>
<td>1</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Y - Decoupled Authentication is supported and preferred if challenge is necessary</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>N - Do not use Decoupled Authentication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_reqdecmaxtime</td>
<td>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.</td>
<td>[0-9]</td>
<td>1</td>
<td>5</td>
<td>o</td>
</tr>
<tr>
<td>3ds_chaccdate</td>
<td>Date that the cardholder opened the account with the merchant. Date format = YYYYYMMDD.</td>
<td>[0-9]</td>
<td>8</td>
<td>8</td>
<td>o</td>
</tr>
</tbody>
</table>
| 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     |
| 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 = YYYYYMMDD.                                             | [0-9] | 8   | 8   | o     |
| 3ds_chacpchangeind| 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     |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>min</th>
<th>max</th>
<th>m/o/c</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_chaccpwchange</td>
<td>Date that cardholder's account with the merchant had a password change or account reset. Date format must be YYYYMMDD.</td>
<td>[0-9]</td>
<td>8</td>
<td>8</td>
<td>o</td>
</tr>
</tbody>
</table>
| 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     |
<p>| 3ds_shipaddressusage      | Date when the shipping address used for this transaction was first used. Date format must be YYYYMMDD. | [0-9] | 8   | 8   | o     |
| 3ds_txnactivityday        | Number of transactions (successful and abandoned) for this cardholder account with the merchant across all payment accounts in the previous 24 hours. | [0-9] | 0   | 10  | o     |
| 3ds_txnactivityyear       | Number of transactions (successful and abandoned) for this cardholder account with the merchant across all payment accounts in the previous year. | [0-9] | 0   | 10  | o     |
| 3ds_provisionattemptsday  | Number of Add Card attempts in the last 24 hours.                            | [0-9] | 0   | 10  | o     |
| 3ds_nbpurchaseaccount     | Number of purchases with this cardholder account during the previous six months. | [0-9] | 0   | 10  | o     |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>min</th>
<th>max</th>
<th>m/o/c</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_suspiciousaccactivity</td>
<td>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</td>
<td>[0-2]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_shipnameindicator</td>
<td>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</td>
<td>[0-2]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_paymentaccind</td>
<td>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</td>
<td>[0-5]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_paymentaccage</td>
<td>Date that the payment account was enrolled in the cardholder’s account with the merchant. Date format must be YYYYMMDD.</td>
<td>[0-9]</td>
<td>8</td>
<td>8</td>
<td>o</td>
</tr>
<tr>
<td>3ds_accid</td>
<td>Additional information about the account optionally provided by the merchant.</td>
<td>[a-zA-Z0-9]</td>
<td>0</td>
<td>64</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_whiteliststatus</td>
<td>Sets the whitelisting status of the merchant. Accepted values are:</td>
<td>[Y, N]</td>
<td>1</td>
<td>1</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>Y - Merchant is whitelisted by cardholder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>N - Merchant is not whitelisted by cardholder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_paytokenind</td>
<td>This field has a value of &quot;true&quot; if the transaction was de-tokenised prior to being received by Credorax.</td>
<td>[a-z]</td>
<td>4</td>
<td>5</td>
<td>o</td>
</tr>
<tr>
<td>3ds_addrmatch</td>
<td>Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are identical. Accepted values:</td>
<td>[a-z]</td>
<td>4</td>
<td>5</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>• True - Shipping Address matches Billing Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• False - Shipping Address does not match Billing Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: the default value of this field is 'false'</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_homephonecountry</td>
<td>Country Code of the home phone.</td>
<td>[0-9]</td>
<td>1</td>
<td>3</td>
<td>o (m if c2 exists)</td>
</tr>
<tr>
<td>3ds_chmobilephone</td>
<td>The mobile phone provided by the Cardholder, without the country code</td>
<td>[0-9]</td>
<td>0</td>
<td>18</td>
<td>o</td>
</tr>
<tr>
<td>3ds_mobilephonecountry</td>
<td>Country Code of the mobile phone.</td>
<td>[0-9]</td>
<td>1</td>
<td>3</td>
<td>o (m if 3ds_chmobilephone exists)</td>
</tr>
<tr>
<td>3ds_chworkphone</td>
<td>The work phone provided by the Cardholder, without the country code</td>
<td>[0-9]</td>
<td>0</td>
<td>18</td>
<td>o</td>
</tr>
<tr>
<td>3ds_workphonecountry</td>
<td>Country Code of the work phone.</td>
<td>[0-9]</td>
<td>1</td>
<td>3</td>
<td>o (m if 3ds_chworkphone exists)</td>
</tr>
<tr>
<td>3ds_shipaddrcity</td>
<td>City of the shipping address requested by the Cardholder.</td>
<td>[a-zA-Z]</td>
<td>3</td>
<td>32</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_shipaddrcountry</td>
<td>Country of the shipping address requested by the Cardholder. Please refer to <a href="#">ISO 3166-1-alpha-2</a> for a list.</td>
<td>[A-Z]</td>
<td>2</td>
<td>2</td>
<td>c</td>
</tr>
<tr>
<td>3ds_shipaddrline1</td>
<td>First line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.</td>
<td>[a-zA-Z]</td>
<td>0</td>
<td>50</td>
<td>o</td>
</tr>
<tr>
<td>3ds_shipaddrline2</td>
<td>Second line of the street address or equivalent local portion of the shipping address associated with the card used for this purchase.</td>
<td>[a-zA-Z]</td>
<td>0</td>
<td>50</td>
<td>o</td>
</tr>
<tr>
<td>3ds_shipaddrpostcode</td>
<td>ZIP or other postal code of the shipping address associated with the card used for this purchase.</td>
<td>[a-zA-Z0-9]</td>
<td>0</td>
<td>16</td>
<td>o</td>
</tr>
<tr>
<td>3ds_shipaddrstate</td>
<td>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.</td>
<td>[0-9]</td>
<td>1</td>
<td>3</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_shipindicator</td>
<td>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:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 - Ship to cardholder's billing address</td>
<td>[0-7]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td></td>
<td>02 - Ship to another verified address on file with merchant. In this case, shipping information is required even though 3ds_addrmatch = true.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04 - &quot;Ship to Store&quot; / 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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>05 - Digital goods (includes online services, electronic gift cards and redemption codes)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>06 - Travel and Event tickets, not shipped</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>07 - Other (for example, Gaming, digital services not shipped, emedia subscriptions, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_deliverytimeframe</td>
<td>Indicates the merchandise delivery timeframe. Accepted values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 - Electronic Delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - Same day shipping</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>03 - Overnight shipping</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>04 - Two-day or more shipping</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0-4] 2 2 o</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_deliveryemailaddress</td>
<td>For electronic delivery, the email address to which the merchandise was delivered.</td>
<td>email</td>
<td>7</td>
<td>64</td>
<td>o</td>
</tr>
<tr>
<td>3ds_reorderitemsind</td>
<td>Indicates whether the cardholder is reordering previously purchased merchandise. Accepted values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 - First time ordered</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - Reordered</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0-2] 2 2 o</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_preorderpurchseind</td>
<td>Indicates whether the cardholder is placing an order for merchandise with a future availability or release date. Accepted values are:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>01 - Merchandise available</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>02 - Future availability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0-2] 2 2 o</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_preorderdate</td>
<td>For a pre-ordered purchase, the expected date that the merchandise will be available.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Date format must be YYYYMMDD.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0-9] 8 8 o</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_giftcardamount</td>
<td>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).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0-9] 1 12 o</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_giftcardcurr</td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[0-9] 3 3 o</td>
<td>-------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_giftcardcount</td>
<td>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.</td>
<td>[0-9]</td>
<td>0</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_purchasedate</td>
<td>Date and time of the purchase expressed in UTC. The field is limited to 14 characters, formatted as YYYYMMDDHHMMSS.</td>
<td>[0-9]</td>
<td>14</td>
<td>14</td>
<td>m</td>
</tr>
<tr>
<td>3ds_recurringexpiry</td>
<td>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</td>
<td>[0-9]</td>
<td>8</td>
<td>8</td>
<td>c</td>
</tr>
<tr>
<td>3ds_recurringfrequency</td>
<td>Indicates the minimum number of days between authorisations. The field is limited to 4 characters. This field is required if a9=1 or 2</td>
<td>[0-4]</td>
<td>0</td>
<td>4</td>
<td>c</td>
</tr>
<tr>
<td>3ds_transtype</td>
<td>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</td>
<td>[0-9]</td>
<td>2</td>
<td>2</td>
<td>m</td>
</tr>
<tr>
<td>3ds_merchantname</td>
<td>Assigned merchant name (with a prefix of &quot;http://&quot; or &quot;https://&quot;)</td>
<td>[a-zA-Z0-9]</td>
<td>1</td>
<td>25</td>
<td>o</td>
</tr>
<tr>
<td>3ds_browseracceptheader</td>
<td>Exact content of the HTTP accept headers. m if 3ds_channel=02</td>
<td>[a-zA-Z0-9]</td>
<td>0</td>
<td>2048</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>d1</td>
<td>IP address of the browser as returned by the HTTP headers. Supports both ipv4 &amp; ipv6 formats.</td>
<td>ip</td>
<td>7</td>
<td>48</td>
<td>o</td>
</tr>
<tr>
<td>3ds_browserjavaenabled</td>
<td>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).</td>
<td>[a-z]</td>
<td>4</td>
<td>5</td>
<td>o</td>
</tr>
<tr>
<td>3ds_browserjavascriptenabled</td>
<td>Boolean that represents the ability of the cardholder browser to execute JavaScript. Accepted values are true / false</td>
<td>[a-z]</td>
<td>4</td>
<td>5</td>
<td>o</td>
</tr>
<tr>
<td>d6</td>
<td>Value representing the browser language as defined in IETF BCP47. For example: en-GB</td>
<td>[A-Za-z,]</td>
<td>2</td>
<td>16</td>
<td>o</td>
</tr>
<tr>
<td>3ds_browsercolordepth</td>
<td>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</td>
<td>[0-9]</td>
<td>1</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_browserscreenheight</td>
<td>Total height of the Cardholder's screen in pixels.</td>
<td>[0-9]</td>
<td>1</td>
<td>6</td>
<td>o</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_browserscreenwidth</td>
<td>Total width of the Cardholder's screen in pixels.</td>
<td>[0-9]</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>m if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3ds_channel=02</td>
</tr>
<tr>
<td>3ds_browsetz</td>
<td>Time difference between UTC time and the Cardholder browser local time, in minutes.</td>
<td>[0-9,-]</td>
<td>1</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>m if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3ds_channel=02</td>
</tr>
<tr>
<td>d5</td>
<td>Exact content of the HTTP user-agent header.</td>
<td>[a-zA-Z0-9]</td>
<td>5</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>m if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3ds_channel=02</td>
</tr>
<tr>
<td>3ds_challengewindowsize</td>
<td>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 &quot;width x height&quot; in pixels. Accepted values are:</td>
<td>[0-5]</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>m if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3ds_channel=02</td>
</tr>
<tr>
<td>3ds_sdkappid</td>
<td>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.</td>
<td>[0-9a-zA-Z]</td>
<td>0</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>m if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3ds_channel=01</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Type</td>
<td>min</td>
<td>max</td>
<td>m/o/c</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----</td>
<td>-----</td>
<td>-------</td>
</tr>
<tr>
<td>3ds_sdkencdata</td>
<td>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.</td>
<td>[0-9a-zA-Z]</td>
<td>0</td>
<td>64k</td>
<td>o</td>
</tr>
<tr>
<td>3ds_sdkephempubkey</td>
<td>Public key component of the ephemeral key pair generated by the 3DS SDK and used to establish session keys between the 3DS SDK and ACS.</td>
<td>[0-9a-zA-Z]</td>
<td>0</td>
<td>255</td>
<td>o</td>
</tr>
<tr>
<td>3ds_sdkmaxtimeout</td>
<td>The maximum amount of time (in minutes) for all exchanges. The value must be greater than or equal to 05.</td>
<td>[0-9]</td>
<td>2</td>
<td>2</td>
<td>o</td>
</tr>
<tr>
<td>3ds_sdkreferencenumber</td>
<td>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.</td>
<td>[0-9a-z]</td>
<td>0</td>
<td>32</td>
<td>o</td>
</tr>
<tr>
<td>3ds_sdktransid</td>
<td>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.</td>
<td>[0-9]</td>
<td>0</td>
<td>36</td>
<td>o</td>
</tr>
</tbody>
</table>
**Response parameters**

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

**Smart 3D Secure Standalone Services**

The Credorax Gateway enables technical and business entities to use the Credorax Smart 3D Secure service as a standalone service. The specifications below guide you on how to use Credorax Smart 3D Secure services if you are connected to the Credorax gateway and process transactions with other acquirers. The specifications also apply if you are connected to the Credorax 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 Credorax 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 Credorax 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]):

<table>
<thead>
<tr>
<th>Field name</th>
<th>Type</th>
<th>M/O</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_merchant_name</td>
<td>String (4,40)</td>
<td>M</td>
<td>The 3DS merchant name as assigned by the acquirer</td>
</tr>
<tr>
<td>3ds_acquirer_bin</td>
<td>Numeric (6,12)</td>
<td>M</td>
<td>The acquirer BIN number</td>
</tr>
<tr>
<td>3ds_acquirer_password</td>
<td>String (8,32)</td>
<td>O</td>
<td>The 3D Secure authentication password as assigned by the acquirer</td>
</tr>
<tr>
<td>3ds_acquirer_mid</td>
<td>String (4,32)</td>
<td>M</td>
<td>The 3D Secure merchant ID as assigned by the acquirer</td>
</tr>
<tr>
<td>3ds_merchant_url</td>
<td>String (4,256)</td>
<td>M</td>
<td>The merchant URL (website)</td>
</tr>
<tr>
<td>3ds_merchant_country</td>
<td>Numeric (3,3)</td>
<td>M</td>
<td>The merchant country</td>
</tr>
<tr>
<td>3ds_merchant_mcc</td>
<td>Numeric (4,4)</td>
<td>M</td>
<td>The merchant category code (MCC) as assigned by the acquirer</td>
</tr>
<tr>
<td>3ds_requestorid</td>
<td>Alphanumeric (35 max)</td>
<td>M</td>
<td>The unique 3D Secure requestor id. Depends on whether you are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Providing 3DS Standalone to Multiple Merchants</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Using 3DS Standalone as a Single Merchant</td>
</tr>
<tr>
<td>3ds_requestorname</td>
<td>Alphanumeric (40 max)</td>
<td>M</td>
<td>The unique 3D Secure requestor name. Depends on whether you are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Providing 3DS Standalone to Multiple Merchants</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Using 3DS Standalone as a Single Merchant</td>
</tr>
</tbody>
</table>
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 Credorax to the partner upon onboarding
  - **{Merchant unique ID}** is a 21-character ID generated by the partner, unique for each merchant

- For Discover: **CREDORAX_{merchant unique ID}**

  Where:
  - **{Merchant unique ID}** is a max 26-character ID generated by the partner, unique for each merchant

Using 3DS Standalone as a Single Merchant

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

- **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 Source 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 the Credorax Source Gateway, you must send the r1 parameter as part of the transaction. The value of the parameter should indicate the processor used for the 3D Secure authentication. A mismatch between the 3DS processor and the transaction processing processor may cause a transaction rejection.

If you only have one processor configured you do not have to provide the 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:

<table>
<thead>
<tr>
<th>ECI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>Mastercard/Maestro authentication is unsuccessful</td>
</tr>
<tr>
<td>01</td>
<td>Mastercard/Maestro authentication attempted</td>
</tr>
<tr>
<td>02</td>
<td>Mastercard/Maestro fully authenticated</td>
</tr>
<tr>
<td>05</td>
<td>Visa/JCB/American Express/Diners/Discover fully authenticated</td>
</tr>
</tbody>
</table>
## ECI Description

<table>
<thead>
<tr>
<th>ECI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td>Visa/JCB/American Express/Diners/Discover authentication attempted</td>
</tr>
<tr>
<td></td>
<td>MasterCard/ Maestro successful authentication (see comment)</td>
</tr>
<tr>
<td>07</td>
<td>Visa/JCB/American Express/Diners/Discover authentication is unsuccessful or</td>
</tr>
<tr>
<td></td>
<td>unattempted, or successfully authenticated (see comment)</td>
</tr>
<tr>
<td></td>
<td>Mastercard/Maestro Recurring Payment fully authenticated</td>
</tr>
</tbody>
</table>

**Comment:** Mastercard/Maestro ECI 06 and Visa ECI with the presence of CAVV value implies that an exemption request was submitted by the acquirer as part of the 3DS 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 Source 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:**

```plaintext
i8=05:0700100908808809000001352980881058cb3a65:3030303030303030303030303030303030353030
i8=06:00000103166177000000003030161770000000000:3030303030303030303030303030303030353030
i8=06:none:202020202020202020202020313531333833303034
```
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 (Merchant Category Code) 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:jJ81HADVRtXICBATEp01CJUAAAA=:00000000000000000501
```

**NOTE:** Attempted Mastercard and Maestro authenticated transactions may not exceed 10% of the total number of Secure Code transactions.

**NOTE:** Source does not participate in the Mastercard/Maestro Advanced Registration and Maestro Recurring Payments Programs and as such does not support Static AAV. The Gateway will thus reject Secure Code transactions 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: AAABAXZhdwAAAMDAWF3AAAAAAA=
```
```
Base-64 decoding (step 1) results in value:
```
awawawaw
```
```
Hex-encoding (step 2) results in value: 00000103166177000000003030161770000000000
```

Guidelines for 3D secure 2.0 and higher

When authentication is done using 3-DSecure 2.0 or higher:
1. The XID sub-field is not required as part of the i8 parameter. Instead send "none".

2. In addition, send the following parameters as part of the request:

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
<th>Format</th>
<th>Min,Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>3ds_version</td>
<td>Indicates the 3D Secure protocol version</td>
<td>[0-9]</td>
<td>3.5</td>
</tr>
<tr>
<td></td>
<td>Possible values:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2.2.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3ds_dstrxid</td>
<td>3DS Directory server transaction ID. Must be sent if 3ds_version = 2.0 or higher and i8 is used.</td>
<td>[0-9A-Za-z-]</td>
<td>34</td>
</tr>
</tbody>
</table>
Appendix K: Ancillary Fee Codes

The following table lists the possible ancillary fee codes that can be sent with parameters `an1` - `an4`.

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Subject/Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.9 rev 2</td>
<td>January 2022</td>
<td>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</td>
</tr>
<tr>
<td>1.9 rev 1</td>
<td>November 2021</td>
<td>Updated Visa requirements for sending all merchant-initiated-transactions with a proper ‘initial transaction id’ (and not a generic value) using the the g6 parameter.</td>
</tr>
<tr>
<td>1.9</td>
<td>November 2021</td>
<td>New functionality: Incremental Authorisation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• New operation code [20]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Updated functionality of request parameters a4 and a9 when used with incremental authorisation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• New response parameter z25 – updated amount</td>
</tr>
<tr>
<td>1.8 rev 12</td>
<td>September 2021</td>
<td>Edited the description of the SmartGuard service</td>
</tr>
<tr>
<td>1.8 rev 11</td>
<td>September 2021</td>
<td>Added a possible value in b21</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed the ISK currency exponent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added parameter z44, response code 79 and result value 07</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Edited the description of special operations 34, 35</td>
</tr>
<tr>
<td>1.8 rev 10</td>
<td>July 2021</td>
<td>Added clarification regarding the a10 parameter</td>
</tr>
<tr>
<td>1.8 rev 9</td>
<td>July 2021</td>
<td>Added response parameters z35, z36, z37</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed max length of c1</td>
</tr>
<tr>
<td>1.8 rev 8</td>
<td>June 2021</td>
<td>Changed token_cavv parameter name to be token_crypto</td>
</tr>
<tr>
<td>Version</td>
<td>Subject/Date</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 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 |
<table>
<thead>
<tr>
<th>Version</th>
<th>Subject/Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.6 rev 2</td>
<td>September 2020</td>
<td>Added new opcodes [88] and [89] allowing to create a token and use a token for 3D Secure authentication-only flow</td>
</tr>
<tr>
<td>1.6 rev 1</td>
<td>August 2020</td>
<td>Changed Optional/Mandatory requirements of Funds Recipient parameters</td>
</tr>
<tr>
<td>1.6</td>
<td>August 2020</td>
<td>Added parameter a1 to opcode [92] mandatory parameters table</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added new parameter a14: partial authorisation tag</td>
</tr>
<tr>
<td>1.5 rev 2</td>
<td>August 2020</td>
<td>Added new response parameter b20 - Payment Account Reference (PAR)</td>
</tr>
<tr>
<td>1.5 rev 1</td>
<td>July 2020</td>
<td>Introduced partial authorisation void</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed Optional/Mandatory requirements of Funds Recipient parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added MCCs relevant for the Referral CFT operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified 3D Secure workflow diagrams</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added new parameter a13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added new Request parameters: Amount Components, Furniture, Car, Plane and Boat Rentals, Event Management, some Travel parameters</td>
</tr>
<tr>
<td>1.5</td>
<td>May 2020</td>
<td>Removed the 3ds_smarplan parameter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of new processing response reason codes</td>
</tr>
<tr>
<td>1.4 rev 4</td>
<td>April 2020</td>
<td>Operation codes clarifications</td>
</tr>
<tr>
<td>1.4 rev 3</td>
<td>April 2020</td>
<td>Minor bug fixes</td>
</tr>
<tr>
<td>1.4 rev 2</td>
<td>March 2020</td>
<td>Addition of new operation result codes</td>
</tr>
<tr>
<td>1.4 rev 1</td>
<td>March 2020</td>
<td>Addition of new Ancillary Fee Codes appendix</td>
</tr>
<tr>
<td>1.4</td>
<td>February 2020</td>
<td>Addition of new travel parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of new parameter h8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of new response parameter z55</td>
</tr>
<tr>
<td>1.3</td>
<td>November 2019</td>
<td>Addition of op codes 104,105 &amp; z51</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Addition of &quot;04&quot; value for 3ds_initiate, and decommission of 3ds_smarstypen parameter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed 3ds_transtype from being Optional to being Mandatory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minor text &amp; formatting corrections</td>
</tr>
<tr>
<td>1.2 rev 4</td>
<td>October 2019</td>
<td>Minor format corrections</td>
</tr>
<tr>
<td>1.2 rev 3</td>
<td>September 2019</td>
<td>Minor format corrections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed the values of Low value exemption &amp; Low Risk Exemption</td>
</tr>
<tr>
<td>1.2 rev 2</td>
<td>July 2019</td>
<td>Clarification on the Hashing algorithm logic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Additional Value &quot;C&quot; for the 3ds_status field</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added required parameter &quot;g1&quot; for op code [38]</td>
</tr>
</tbody>
</table>
### 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@credorax.com