Web Services Guide

For Third Party Tokenisation Service Providers

Version: 1.1
05 April 2023

Publication number: TPWSG-1.1-4/5/2023

Global Processing Services
6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Support Email: ops24@globalprocessing.com
Support Phone: +442037409682

For the latest technical documentation, see the Documentation Portal.

Copyright

About this Guide

This guide is intended as a reference guide, to provide information on the available GPS web services and fields in each web service, for third party tokenisation service providers who offer services to GPS customers and who need to use the GPS web services API to integrate their service.

Target audience

This guide is aimed at third party developers who need to integrate their service to GPS. You should know how to implement SOAP-based calls and handle the response.

Note: If you are undertaking full card management on behalf of Program Managers (e.g., creating cards, loading cards and changing card status), please refer to the full Web Services Guide.

What's changed?

If you want to find out what's changed since the previous release, see the Document History section.

How to use this Guide

Before you start:

- Make sure you can connect to the GPS web service, by implementing a simple call, as explained in Using the API.

Implementing web service calls

- When implementing a web service request, you must at a minimum include the mandatory request fields and handle the fields that are mandatory in the response.
- Where a field requires you to submit a code value or returns a code value, the guide provides links to the relevant appendix for details. If in doubt as to which code to include in your request, you should use the default or recommended value.
- Do not change the default xmlns attributes (XML namespaces) in the SOAP request.
- Don't use spaces in xml tags.
- Please pay particular attention to XML tag name spelling and capitalisation. Different web services may sometimes adopt different case and naming conventions. If in doubt, always refer to the GPS-provided SOAP WSDL. See Using the API.

Conventions used in this Guide

When reading the tables in this guide, note the following information is provided for each XML field:

Element	Description
Tag	The XML tag name. Please pay particular attention to the capitalisation and spelling. Where a tag name is used within text, this is formatted as in the following example: <ActionCode>
Type	The type of field value supported. Options include: N = number AN = alpha-numeric YYYY-MM-DD = date format: Year-Month-Date HHMMSS = time format: Hour-Minute-Second D = decimal B = boolean
Minimum / Maximum Length	The allowed minimum and maximum field length. If in doubt, refer to the WSDL or examples provided in the guide.
Request / Response	The status of the field in the request and response. Options are: Mandatory = must be included in the request and will be in the response

Element	Description
	Conditional = this field is mandatory under specified conditions. Refer to the description for details. Optional = can be included. May be in the response. Omit = you should omit this field. Will not be in the response

Other Documentation

Refer to the table below for a list of other relevant customer documents that should be used together with this guide.

Document	Description
Tokenisation Service Guide	Guide for GPS customers, which provides details of the GPS payment tokenisation service, using MDES (Mastercard) or VDEP (Visa).
Web Service Guide	Guide for GPS customers, which provides details of the available GPS web services and how to use them.

Tip: For the latest technical documentation, see the Documentation Portal.

Overview

The GPS web service is based on SOAP Version 1.1.

SOAP (Simple Object Access Protocol) is a messaging protocol for exchanging structured information in the implementation of web services. It uses Extensible Markup Language (XML) for its message format and relies on application layer protocols such as HTTP for message negotiation and transmission. SOAP allows developers to invoke processes running on disparate operating systems (such as Windows, macOS, and Linux) to authenticate, authorise and communicate using XML.

The figure below describes how the web services API is used to integrate external systems to GPS.

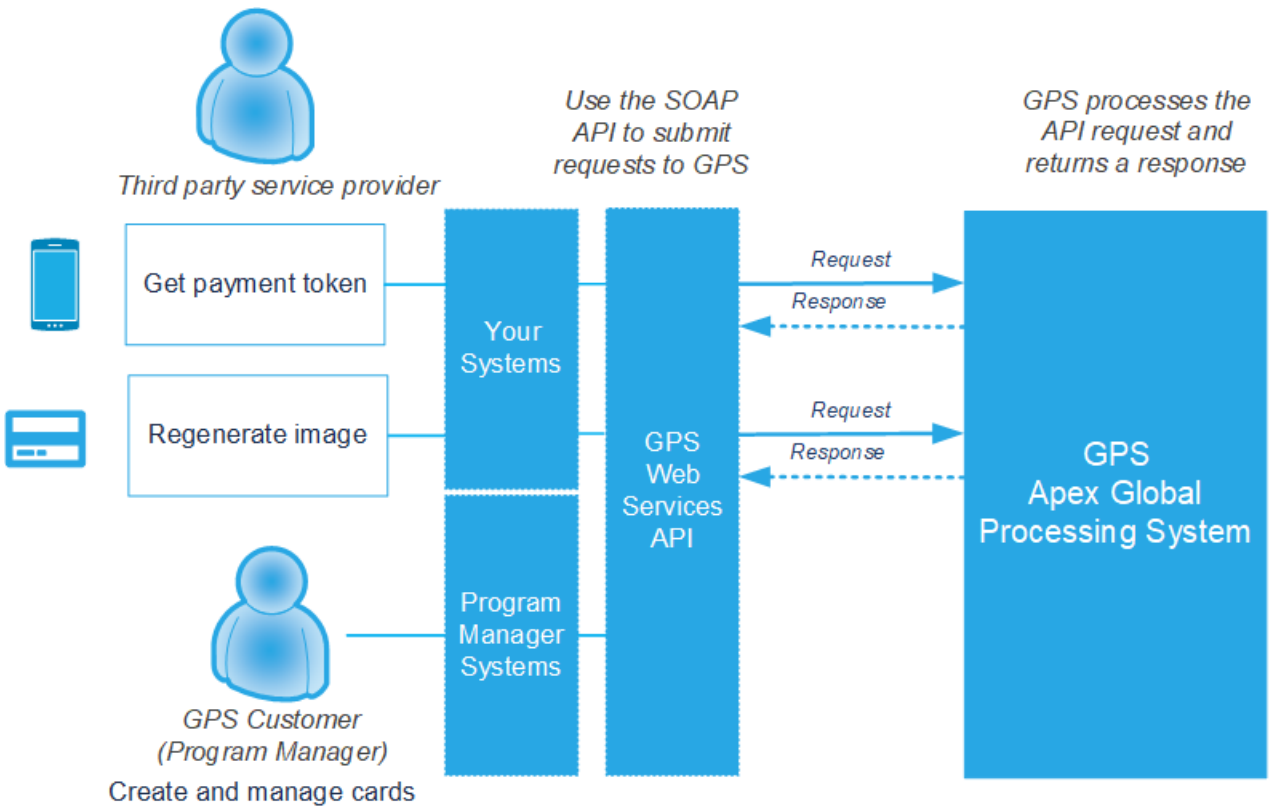

Figure 1: Figure: API Architecture Overview

Note: Third party integrators may require a different URL to access the SOAP Web Services. This will be confirmed during your project setup phase.

Using the API

This section provides tips on how to integrate to GPS using the SOAP web services API.

Using the Web Services

View the WSDL

You can open the following URL in a browser to view the structure of the WSDL:

https://ws-uat.globalprocessing.net:13682/service.asmx?WSDL

If you are a third party integrator providing services such as tokenisation or virtual card setup, you will require a dedicated URL. This will be confirmed during the project setup phase.

> **Tip:** We recommend you always refer to the WSDL for the correct XML tag name spelling and capitalisation, as different web services may sometimes adopt different case and naming conventions.

Install a SOAP Application

We recommend that you use an API tool that supports SOAP to test out the GPS web services.

SOAPUI is an open-source application, which you can download and install on any computer, which enables you to submit test transactions to GPS.

Load the SOAP WSDL

You can load the GPS SOAP test WSDL into your SOAP tool. If you are using SOAPUI, then:

1. Select **File > New SOAP Project**.
2. Enter a project name and then, in the **Initial WSDL** field, paste the following URL: https://ws-uat.globalprocessing.net:13682/service.asmx?WSDL
3. Click **OK**.

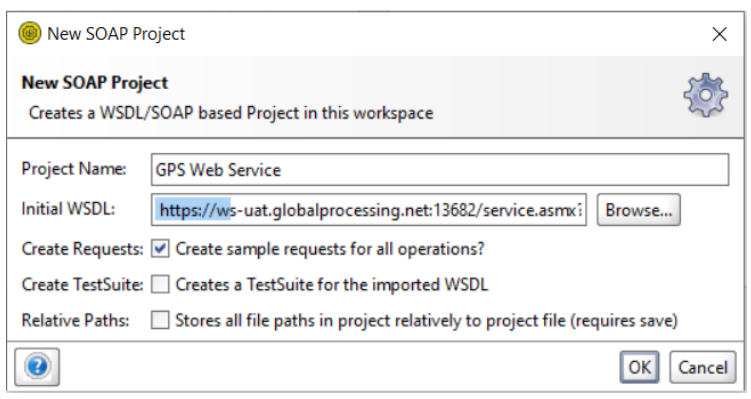

Figure 2: Figure: Starting a new SOAP project and importing the WSDL

Implementing a SOAP Request

Always follow the instructions provided for Implementing web service calls, to ensure that your XML requests are correctly formated.

You can implement a SOAP call as follows:

1. Select a SOAP service from the left-hand navigation pane. We recommend you start with a check of the status of the web service to make sure you can connect, using `Ws_Check`. See Check Service Availability.
2. In the centre pane, customise the SOAP details of your transaction. At a minimum, you will need to enter your username, password and Issuer Code (`IssCode`). If you don't have these details, check with you GPS Implementation Manager.

   > **Tip:** You can copy and paste examples in this guide into the SOAP window, and customise as required.

3. Click **Submit**.

The SOAP response should be displayed in the right-hand pane within SOAPUI. A successful request will return an ActionCode status of *000* (Normal, approved). See Action Codes.

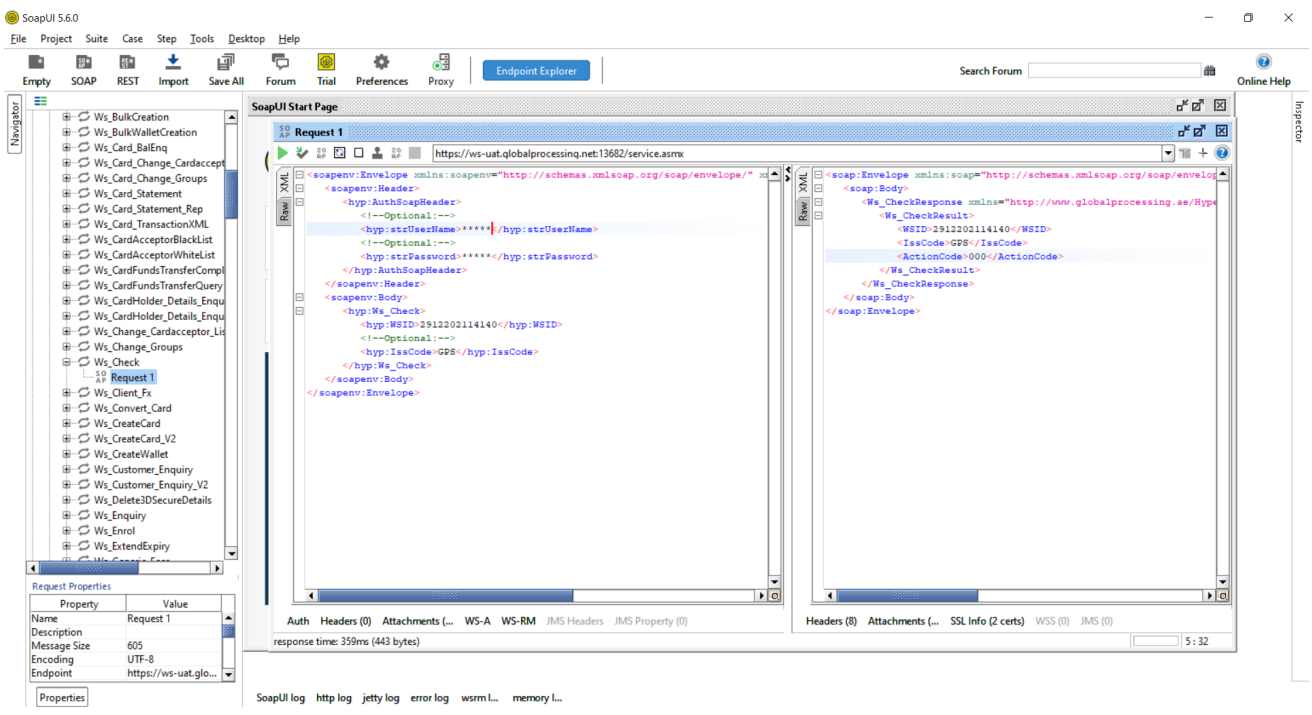

Figure 3: Figure: Example of a SOAP Request in SOAPUI

Fair Usage Policy

GPS has a Fair Usage Policy which restricts the maximum number of *concurrent* web service connections per client (IP address) to 20.

If you send more than 20 concurrent web service requests to GPS an HTTP error message 403, sub-status 501 is returned. This can be mitigated by controlling your outbound web server configuration. For further details, please contact your Implementation Manager or Account Manager.

Introduction to the Web Services API

The table below lists the web services available to third party tokenisation service providers (ordered alphabetically).

API	Description
Ws_Check	Checks web service availability. It validates the SOAP credentials and Issuer Code by calling database procedures.
Ws_Payment_Token_Get	Gets the details for MDES (Mastercard Digital Enablement Service) Payment Token Cards.
Ws_Regenerate	Retrieves the card image configured in the GPS platform for virtual and physical cards that have been converted which can then be displayed to the cardholder. If a customer wants to see the image some time after card creation you can regenerate the image. This web service can also be used to replace Lost or Stolen cards; the customer will be issued with a new PAN, CVV2 and Expiry Date.

Note: This is a small subset of the available GPS web services API. For a full list of the API available to GPS customers to manage their card program, refer to the Web Services Guide.

Check Service Availability

API: Ws_Check

This web service is used to check web service availability. It validates the SOAP credentials and Issuer Code.

Note: GPS has extensive automated monitoring of web services availability and response times. Our current annual service availability is over 99.96%.

Record Description

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<WSID>	N	1	19	Web service ID. Unique for every request.	Mandatory	Mandatory
<IssCode>	AN	1	4	GPS Issuer (Program Manager) Code. Assigned by GPS.	Mandatory	Mandatory
<ActionCode>	AN	3	3	The action code for the response. See Action Codes. If the web service is available, returns “000”.	Omit	Mandatory

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
   <soapenv:Header>
      <hyp:AuthSoapHeader>
         <hyp:strUserName>******</hyp:strUserName>
         <hyp:strPassword>******</hyp:strPassword>
      </hyp:AuthSoapHeader>
   </soapenv:Header>
   <soapenv:Body>
      <hyp:Ws_Check>
         <hyp:WSID>2021123456789</hyp:WSID>
         <hyp:IssCode>PMT</hyp:IssCode>
      </hyp:Ws_Check>
   </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="h-
ttp://www.w3.org/2001/XMLSchema">
   <soap:Body>
      <Ws_CheckResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
         <Ws_CheckResult>
            <WSID>2021123456789</WSID>
            <IssCode>PMT</IssCode>
            <ActionCode>000</ActionCode>
         </Ws_CheckResult >
      </ Ws_CheckResponse>
   </soap:Body>
</soap:Envelope>
```

Card Regenerate Image

API: Ws_Regenerate

This web service enables you to retrieve the card image configured on the GPS platform, which can then be displayed to the cardholder. Card images are stored for both virtual cards and physical cards that have been converted from virtual cards. If a customer wants to see the image some time after card creation you can regenerate the image by using this web service.

Record Description

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<PublicToken>	AN	1	9	The card's public token. Mandatory in request and response.	Mandatory	Mandatory
<RegenType>	N	1	1	Whether to regenerate the card. 0 = only return the CVV and do not regenerate; 1 = Regenerate the card only if it has a status of lost or stolen, else recreate the card image (note: legacy only, use Ws_Renew_Card. See Card Renew); 2 = Only create the card image, do not regenerate card.	Mandatory	Omit
<Sms_ Required>	N	1	1	Whether an SMS is sent to the cardholder with the card's CVV. 1 = yes; 0 =No. The default is '0'. The SMS is configurable.	Mandatory	Omit
<Sms_Content >	N	1	1	Reserved for future use; set to 0.	Mandatory	Omit
<CVV>	AN	3	3	Card Verification Value, the 3-digit code printed on the back of the card.	Omit	Mandatory
<ActionCode>	AN	3	3	The action code for the response. See Action Codes.	Omit	Mandatory
<Image>	Base64 Binary			PGP-encrypted image of the card. Is only returned if a PGP key has been shared and configured.	Omit	Conditional
<ExternalRef>	AN	1	30	External reference code for the card. **Note**: Legacy field. Not used.	Optional	Omit
<TerminalID>	AN	1	15	Point of Sale (POS) or other terminal identifier, such as a hostname.	Optional	Omit
< MailOrSMS>	AN	1	1	The cardholder's preferred contact method. 0 = SMS; 1 = email. 2 = SMS and email. Default value is '0'.	Optional	Omit
<CustAccount>	AN	1	25	Cardholder account number or reference number. You can use this reference to find the cards linked to a cardholder. Also displayed in Smart Client as *Customer Reference*.	Optional	Optional
<PAN>	N	16	19	Card Number displayed as masked. **Note**: For customers who are PCI DSS Compliant, the full PAN can be returned if required. This must be enabled at Program Manager level and will apply to all web services which return the PAN. Only returned for successful calls.	Omit	Conditional
<WSID>	N	1	19	Web service ID. Unique for every request.	Optional	Omit
<IssCode>	AN	1	4	GPS Issuer (Program Manager) Code. Assigned by GPS.	Optional	Omit
<FeeWaiver>	N	1	1	Indicates whether to waive any web service fee set up on the system: 0 = No, 1=Yes. Default is	Optional	Omit

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
				0.		

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
   <soapenv:Header>
      <hyp:AuthSoapHeader>
         <hyp:strUserName>******</hyp:strUserName>
         <hyp:strPassword>******</hyp:strPassword>
      </hyp:AuthSoapHeader>
   </soapenv:Header>
   <soapenv:Body>
      <hyp:Ws_Regenerate>
         <hyp:PublicToken>123456789</hyp:PublicToken>
         <hyp:RegenType>1</hyp:RegenType>
         <hyp:Sms_Required>0</hyp:Sms_Required>
         <hyp:Sms_Content>0</hyp:Sms_Content>
         <hyp:ExternalRef>ABCD001</hyp:ExternalRef>
         <hyp:TerminalID>POS-TEST</hyp:TerminalID>
         <hyp:MailOrSMS>0</hyp:MailOrSMS>
         <hyp:WSID>2021123456789678</hyp:WSID>
         <hyp:IssCode>CLIENT</hyp:IssCode>
      </hyp:Ws_Regenerate>
   </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="h-
ttp://www.w3.org/2001/XMLSchema">
   <soap:Body>
      <Ws_RegenerateResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
         <Ws_RegenerateResult>
            <PublicToken>123456789</PublicToken>
            <ActionCode>000</ActionCode>
            <CVV>123</CVV>
            <PAN>123456******4321</PAN>
         </Ws_RegenerateResult>
      </Ws_RegenerateResponse>
   </soap:Body>
</soap:Envelope>
```

Payment Token Get

API: Ws_Payment_Token_Get

This web service gets the details for both Mastercard Digital Enablement Service (MDES) payment token cards and Visa Token Service (VTS) cards.

Your request must provide one of the following card details: PAN, PublicToken, DPAN or Payment_Token_ID. If the MDES or VTS card is not specified, the call returns all linked MDES or VTS cards.

Record Description

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<WSID>	N	1	19	Web service ID. Unique for every request.	Mandatory	Mandatory
<IssCode>	AN	1	4	GPS Issuer (Program Manager) Code. Assigned by GPS. If only <IssCode> is present in the request then this method returns the pending fee details of all cards belong to the given program manager.	Mandatory	Mandatory
<TxnCode>	AN	1	2	The Transaction Code. See Transaction Codes. Default value is 9.	Mandatory	Mandatory
<PAN>	N	16	19	Card Number. Unique card identifier.	Conditional	Omit
<PublicToken>	N	9	9	GPS 9-digit public token of the card.	Conditional	Omit
<DPAN>	AN	16	19	Digital PAN value for the card.	Conditional	Omit
<Payment_ Token_ID>	N	1	20	Payment token identifier for the MDES or VTS Card.	Conditional	Omit
<LocDate>	YYYY-MM-DD	10	10	The local current date in *year-month-date* format.	Mandatory	Mandatory
<LocTime>	HHMMSS	6	6	The local current time, in *hour-minute-second* format.	Mandatory	Mandatory
<ActionCode>	AN	3	3	The action code for the response. See Action Codes.	Omit	Mandatory

Payment Token Get Res Info

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<Creator>	AN	1	10	Name of the system or process that created the token (e.g., MC-MDES and VISA-T).	Omit	Mandatory
<Creator_ PAN_Ref>	AN	1	48	The token creator's unique reference to the linked card.	Omit	Mandatory
<Creator_ Token_Ref>	AN	1	48	The token creator's unique reference for this payment token. (Mastercard Token Unique Reference (TUR) and Visa Token reference ID.)	Omit	Mandatory
<PANT>	N	16	19	PAN for the card linked to the MDES or VTS card.	Omit	Mandatory
<Payment_ Token >	N	16	19	Payment token Device PAN for the MDES or VTS card.	Omit	Mandatory
<Payment_ Token_ ExpDate >	Date	10	10	Expiry date of the payment token.	Omit	Mandatory
<Payment_ Token_ID>	N	1	20	Payment token identifier for the MDES or VTS card.	Omit	Mandatory
<Payment_ Token_Type >	AN	1	2	Payment token type. See Payment Token Types.	Omit	Mandatory
<Wallet_ID>	AN	1	10	Name of the wallet provider this payment token uses (e.g., APPLE, ANDROID, SAMSON).	Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<GPS_Status>	N	2	2	The GPS status of the payment token for transacting. See Status Codes.	Omit	Mandatory
<Tokenised_ Datetime>	DateTime	19	19	Date and time when tokenised, in the format: *yyyy-mm-ddhhmmss*.	Omit	Mandatory
<Tokenised_ Status>	AN	1	1	Tokenised status of this payment token: U = unknown; 0 = not tokenised; 1=tokenised.	Omit	Mandatory
<Txn_Status>	AN	1	1	Status of the payment token as received from the payment token creator (normally Visa or Mastercard). After tokenisation, this is not changed by GPS. A = Active D = Deleted (once in this status, it is normally never changed) I = Inactive N = Not Tokenised P = Pending S = Suspended U = Unknown X = Deactivated	Omit	Mandatory
<Txn_Status_ Actor>	AN	1	10	Indicates which system last changed the transaction status.	Omit	Mandatory
<Txn_Status_ Change_ Datetime>	DateTime	16	16	Date and time that the transaction status was last changed. In the format: *yyyy-mm-ddhhmmss*.	Omit	Mandatory
<Accepted_ Terms_Date_ GMT>	DateTime	16	16	Date (in GMT) that terms and conditions were accepted by the cardholder (as received from the network).	Omit	Mandatory
<Accepted_ Terms_ Version>	AN	1	32	Version of the terms and conditions which were accepted by the cardholder (as received from the network).	Omit	Mandatory
<Auth_ Datetime>	DateTime	16	16	Date and time when the tokenisation request was last responded to.	Omit	Mandatory
<Auth_ Decision>	AN	1	1	Final tokenisation decision: U = unknown 0 = approve digitisation request A = approve digitisation request (with additional authentication).	Omit	Mandatory
<Auth_ RSPSRC>	AN	10	10	Name of the system or process that approved the tokenisation (e.g., MC-MDES and ISSUER).	Omit	Mandatory
<Auth_Status>	AN	1	1	Status of the authorisation to digitise this payment token: U = unknown 0 = approve digitisation request A = approve digitisation request (with additional authentication) 1 = decline digitisation request **Note**: this is not the same as a transaction authorisation.	Omit	Mandatory
<Digitisation_ Ref>	AN	1	64	Unique reference (per payment_token_issuer_id) which all digitisation messages use, to link them together.	Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
<Wallet_ Account_ Score>	N	1	1	Risk score for the account, received from the wallet provider during digitisation: 1 = highest risk; 2 = higher risk 3 = neutral; 4 = lower risk; 5 = least risk	Omit	Mandatory
<Wallet_ Device_Score>	N	1	1	Risk score for the device received from the wallet provider during digitisation: 1 = highest risk; 2 = higher risk 3 = neutral; 4 = lower risk; 5 = least risk	Omit	Mandatory
<Wallet_ Reasons>	AN	1	24	Wallet service provider tokenization recommendation reason codes. See Wallet Tokenisation Reason Codes.	Omit	Mandatory
<Activation_ Code>	AN	1	40	Activation code to be sent directly to the cardholder to activate this payment token.	Omit	Mandatory
<Activation_ Code_Expdate	DateTime	16	16	Date and time when the activation code expires, in GMT (UTC). In the format: *yyyy-mm-ddhhmmss*.	Omit	Mandatory
<Activation_ Method>	N	1	1	Which activation method was used: 0 = none; 1 = SMS to mobile phone; 2 = email; 3 = cardholder called an automated call centre; 4 = cardholder called a human call centre; 5 = website; 6 = mobile application; 7 = voice phone call	Omit	Mandatory
<Device_ID>	AN	1	48	Unique ID of the secure element in the device.	Omit	Mandatory
<Device_IP>	AN	1	15	IP address (full or last part only) of the device at time of binding / digitisation.	Omit	Mandatory
<Device_ Lang2>	AN	1	2	Device language code as ISO 639-1 (2 letter lowercase) code.	Omit	Mandatory
<Device_ Latitude>	N	1	3	Device latitude in degrees at time of digitisation request: -90 (south pole) to +90 (north pole). +ve=North, -ve=South (from equator). Example: +63.2 = North 63.2 degrees, -82.6 = South 82.6 degrees.	Omit	Mandatory
<Device_ Longitude>	N	1	3	Device longitude in degrees at time of digitisation request: -180 to +180; +ve = East, -ve = West (of Greenwich). Example: 176.2 = East 176.2 degrees, -98.5 = West 98.5 degrees.	Omit	Mandatory
<Device_ Name>	AN	1	20	Name the cardholder assigned to the device in the wallet.	Omit	Mandatory
<Device_Tel_ Num>	AN	1	15	Device telephone number (full or last part only).	Omit	Mandatory
<Device_Type>	AN	1	1	The type of device used at the terminal. See Device Types.	Omit	Mandatory
<FirstName>	AN	1	40	Cardholder's first name as provided by the wallet provider during digitisation. May not be provided, or just the initial letter.	Omit	Mandatory
<LastName>	AN	1	40	Cardholder's last name as provided by wallet	Omit	Mandatory

Tag	Type	Minimum Length	Maximum Length	Description	Request	Response
				provider during digitisation. May not be provided, or just the initial letter.		
<Wallet_ Account_ Hash>	AN	1	64	Wallet provider hash of account details (optional)or PBKDF2 hash of the cardholder's account ID with the wallet provider.	Omit	Mandatory

Request

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:hyp="http://www.globalprocessing.ae/HyperionWeb">
   <soapenv:Header>
      <hyp:AuthSoapHeader>
         <hyp:strUserName>******</hyp:strUserName>
         <hyp:strPassword>******</hyp:strPassword>
      </hyp:AuthSoapHeader>
   </soapenv:Header>
   <soapenv:Body>
      <hyp:Ws_Payment_Token_Get>
         <hyp:WSID>202112345678967890</hyp:WSID>
         <hyp:IssCode>PMT</hyp:IssCode>
         <hyp:TxnCode>2</hyp:TxnCode>
         <hyp:PAN></hyp:PAN>
         <hyp:PublicToken>123456789</hyp:PublicToken>
         <hyp:DPAN>0987654321012</hyp:DPAN>
         <hyp:Payment_Token_ID></hyp:Payment_Token_ID>
         <hyp:LocDate>2017-01-01</hyp:LocDate>
         <hyp:LocTime>123456</hyp:LocTime>
      </hyp:Ws_Payment_Token_Get>
   </soapenv:Body>
</soapenv:Envelope>
```

Response

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="h-
ttp://www.w3.org/2001/XMLSchema">
   <soap:Body>
      <Ws_Payment_Token_GetResponse xmlns="http://www.globalprocessing.ae/HyperionWeb">
         <Ws_Payment_Token_GetResult>
            <WSID>202112345678967890</WSID>
            <IssCode>PMT</IssCode>
            <TxnCode>2</TxnCode>
            <PublicToken>123456789</PublicToken>
            <PaymentTokenGetResInfo>
               <PaymentTokenGetResInfo>
                  <Creator>GPS</Creator>
                  <Creator_PAN_Ref/>
                  <Creator_Token_Ref/>
                  <PANT>1234567890123456</PANT>
                  <Payment_Token>*****1234</Payment_Token>
                  <Payment_Token_ExpDate/>
                  <Payment_Token_ID>2</Payment_Token_ID>
                  <Payment_Token_Type>C</Payment_Token_Type>
                  <Wallet_ID>APPLE</Wallet_ID>
                  <GPS_Status>00</GPS_Status>
                  <Tokenised_Datetime/>
                  <Tokenised_Status>1</Tokenised_Status>
                  <Txn_Status>X</Txn_Status>
                  <Txn_Status_Actor></Txn_Status_Actor>
                  <Txn_Status_Change_Datetime/>
                  <Accepted_Terms_Date_GMT/>
                  <Accepted_Terms_Version/>
                  <Auth_Datetime/>
                  <Auth_Decision/>
                  <Auth_RSPSRC/>
                  <Auth_Status>1</Auth_Status>
                  <Digitisation_Ref>11111111111111</Digitisation_Ref>
                  <Wallet_Account_Score/>
                  <Wallet_Device_Score/>
                  <Wallet_Reasons/>
                  <Activation_Code/>
                  <Activation_Code_Expdate/>
                  <Activation_Method/>
```

```
                  <Device_ID/>
                  <Device_IP/>
                  <Device_Lang2/>
                  <Device_Latitude/>
                  <Device_Longitude/>
                  <Device_Name/>
                  <Device_Tel_Num/>
                  <Device_Type>M</Device_Type>
                  <FirstName/>
                  <LastName/>
                  <Wallet_Account_Hash/>
               </PaymentTokenGetResInfo>
            </PaymentTokenGetResInfo>
            <LocDate>2017-01-01</LocDate>
            <LocTime>123456</LocTime>
            <SysDate>2017-11-17</SysDate>
            <ActionCode>000</ActionCode>
         </Ws_Payment_Token_GetResult>
      </Ws_Payment_Token_GetResponse>
   </soap:Body>
</soap:Envelope>
```

Appendices Overview

This section contains a list of appendices with further reference information. See the table below.

Appendix	Description
Action Codes	Action codes returned by GPS in response to a request.
Transaction Codes	Transaction codes used in a web service response.
SMS Configuration Options	Options for configuring the SMS messages sent to your customers.
Status Codes	Codes that represent the status of a card.
Transaction Types	Codes that represent the transaction type.
Transaction Status	Codes that represent the transaction status.
Payment Token Types	Payment token types.
String Cleaning and Approved Characters.	Details of special characters that are removed from input fields and approved characters for use on cards.
Processing Codes (DE003)	Description of processing codes returned in the `<ProcCode>` field for a Card Statement request.
Currency Codes	List of currency codes and their exponents.

Action Codes

The following action codes may be returned in the <ActionCode> tag of a web service response.

Code	Description	How is it used?
000	Normal, approve	Indicates success of the web service transaction.
100	Do not Honour, deny	As required by Issuer. Also used for example in Card Load when the currency in the request does not match the card currency.
101	Card expired, deny	Used to check expiry status of card before allowing certain operations e.g. Load.
104	Restricted card, deny	Used to indicate that the card is in restricted status (41,43,62 or 14).
105	Call acquirer security, deny	As required by Issuer
106	PIN tries exceeded, deny	As required by Issuer
107	Refer to issuer, deny	As required by Issuer
116	Insufficient funds, deny	Used to indicate lack of funds to the account, e.g., to cover the fee associated with the request.
118	No card record, deny	Used to indicate the PAN/Pubtoken/CustAccount/AccountID in the request has no associated card record in the database.
119	Transaction not allowed to cardholder, deny	Used to indicate that the cardholder is not allowed to perform that particular transaction type.
120	Action will exceed allowed system limit	Used when any of the card or account amount system limits are exceeded.
121	Amount limits exceeded or outside valid load range, deny	Used when any of the card or account amount limits are exceeded or a load amount falls outside the valid range.
122	Invalid ExternalAuth	Incorrect External Authorisation (ExternalAuth) value. Possible values are: 0 and 1. Empty value defaults to 0. See Card Create > ExternalAuth.
123	Frequency limits exceeded, deny	Used when any of the card or account frequency limits are exceeded.
124	Card already active, deny.	Used when an active card is tried to be activated again.
125	Card not effective, deny	Used when the card has not yet been activated.
126	Invalid PIN, deny	Used to indicate that the supplied PIN does not match our records.
127	No CVC2 tries remaining limit found for the card	Used to indicate that the allowed number of CVC2 tries has been reached.
130	External API unreachable	Used when an external API is called e.g. ws_ PINControl when Func=06.
131	External API returned an error	Used when an external API is called e.g. ws_ PINControl when Func=06, and an error is returned. For the actual error, contact GPS or the external API provider.
140	Invalid Currency. Currency doesn't match with product configuration.	Indicates a product and currency mismatch for a SEPA payment (when using the Modulr Agency Banking service).

Code	Description	How is it used?
141	MandateId is missing.	Modulr (Agency Banking Service)
142	Cancellation Code is missing or invalid.	Modulr (Agency Banking Service)
144	No entry in the database for the input MandateId.	Modulr (Agency Banking Service)
145	No mandate details found.	Modulr (Agency Banking Service)
167	No PIN assigned, deny	Used when trying to retrieve a PIN from a card that has no PIN assigned.
168	PIN already present, deny	Used when trying to set a PIN on a card that already has a PIN assigned.
169	No-PIN card, deny	Used when requesting a PIN on a card that is marked as a 'no-PIN' card.
184	PIN confirmation failed, deny	Used when the PIN confirmation does not match the new PIN when attempting to change the PIN.
200	Card closed, deny & pickup	As required by Issuer
202	Fraudulent use, deny & pickup	As required by Issuer
204	Restricted card, deny & pickup	As required by Issuer
205	Call acquirer security, deny & pickup	As required by Issuer
206	PIN tries exceeded, deny & pickup	As required by Issuer
207	Special conditions, deny & pickup	As required by Issuer
208	Card lost, deny & pickup	Used to indicate that the card is in Lost status (41).
209	Card stolen, deny & pickup	Used to indicate that the card is in Stolen status (43).
210	Invalid DPAN	Used to indicate that the supplied tokenised PAN is invalid.
211	Invalid Payment Token Id	Used to indicate that the supplied Payment Token id is invalid.
212	Card and Payment Token details do not match	Used to indicate that the supplied Card details and Payment Token do not relate.
213	FPAN status change is successful. DPANs are ignored as they are in irreversible status.	The FPAN was successfully updated, but the DPAN was not updated, as it is in an irreversible status.
214	No associated Payment Token for the card details supplied	There is no associated Payment Token for the card details supplied.
216	Either DPAN or PaymentTokenId must be provided	Provide a valid DPAN or PaymentTokenId
217	Invalid Func value	Provide a valid value, such as: 00 and 01.
218	Payment token has no device in the list	No associated device in the system.
219	Specified device index is not in the list	No Visa device index exists that matches the supplied value of <DeviceIndex>.
220	The device is already in unbound status	You made can attempt to unbind a device that is not bound to any DPAN,
221	DeviceIndex is mandatory when value of Func is '01'.	For Token Device Management (Ws_Token_Device_Management), when the token device function requested is to unbind the device, then the Visa device index should be provided.
250	Banking balance transfer not allowed on account status	BOTTOM LINE (AGENCY BANKING SOLUTION)
400	Addrl1 is missing, Addrl1 is mandatory if 'Address' fields are being specified.	Reserved for future use
401	Invalid PostCode	Postcode is not formed from alphanumerics or hyphens

Code	Description	How is it used?
402	dlvaddr1 is missing, dlvaddr1 is mandatory if 'Delivery Address' fields are being specified.	Reserved for future use
403	Invalid dlvpostcode	Postcode is not formed from alphanumerics or hyphens.
404	Workaddr1 is missing, Workaddr1 is mandatory if 'Work Address' fields are being specified.	Reserved for future use
405	Invalid Workpostcode	Postcode is not formed from alphanumerics or hyphens.
406	Invalid IssCode	IssCode does not match the credentials supplied.
409	Invalid PAN, PAN must be composed of digits	Used when PAN is not a valid number composed of digits.
410	Invalid PublicToken, PublicToken must be composed of digits	Used when PublicToken is not a valid number composed of digits.
411	Invalid NewPAN, NewPAN must be composed of digits	Used when NewPAN is not a valid number composed of digits.
412	Invalid NewToken, NewToken must be composed of digits	Used when NewToken is not a valid number composed of digits.
413	Invalid PrimaryToken, PrimaryToken must be composed of digits	Used when PrimaryToken is not a valid number composed of digits.
414	Invalid MVCToken, MVCToken must be composed of digits	Used when MVCToken is not a valid number composed of digits.
415	Invalid CardDesign, CardDesign must be composed of digits	Used when CardDesign is not a valid number composed of digits.
416	Could not complete request, partial results returned	Used when not all requests within a bulk operation could be completed.
418	Both allow list and deny list are present in the request. Customer can only assign either allow list or deny list to a card	Used when both request parameters are supplied, only one is allowed.
419	Invalid RenewOptions	Indicates an invalid RenewOption was supplied.
420	NewProductID not present in the request	Indicates the request parameter was missing.
421	Invalid ExpiryDate format, it should be YYYY-MM-DD	Indicates the request parameter was in an invalid format.
422	Card request has been taken into account by the system. The production files are not yet generated.	Indicates a card renewal is already in progress.
423	This card request has been already processed and the production files are successfully generated.	Indicates a card renewal is already in progress.
424	This card has an expiry less than one month, which is less than minimum validity. Please select a RenewOptions other than 0,2 and 4.	Indicates an attempt to renew card thar is about to expire, without supplying a new expiry date.
425	Invalid AccumulatorType	Indicates the supplied parameter was an invalid value.
426	New available to spend balance on card is greater than new current balance on the card. The new available to spend balance should be less than new current balance.	Indicates the supplied parameter was an invalid value.
427	Balance stand-in not enabled in External Host Settings	Indicates the card is not valid for the operation.
431	Invalid PaymentTokenUsageGroup has been supplied, should be numeric.	Indicates the supplied parameter was an invalid value.
432	Incorrect PaymentTokenUsageGroup. (Returns when the group code is not present in GPS database)	Indicates the supplied parameter was an invalid value

Code	Description	How is it used?
433	Invalid Delivery Method has been supplied, should be numeric.	Indicates the supplied parameter was an invalid value
434	Credential Value is missing, should be supplied when Action is add or update.	Returned in a 3D Secure request to add a credential to a card. See 3D Secure RDX Credentials (Cardinal).
435	Incorrect Virtual Card Image.	Returned when the Virtual Card Image ID is not present in GPS database.
436	Incorrect Image Size.	Returned when the Size is not present in GPS database.
437	No credentials found for the token.	Returned in response to a GET request for the 3D Secure credentials linked to a card if no credentials are found. See 3D Secure RDX Credentials (Cardinal).
438	Credential type already exists for this token.	Returned in response to an Add request if the credential type already exists for this card.
439	Value supplied is not valid	Returned in response to a create token request (Ws_PaymentToken_Create) where an invalid value is provided.
440	Archived card, deny	If the request relates to an archived card record, the request is denied. (Applies to the following web services: Create_Card, Create_Wallet, Regenerate, Regenerate_Wallet and ws_Renew.)
441	Value not supplied for mandatory field	Returned in response to a service request where a mandatory field is empty.
442	Data supplied is in invalid format	Returned in response to a create token request (Ws_PaymentToken_Create) where a value is provided in an incorrect format.
443	Default value is not set	Returned in response to a create token request (Ws_PaymentToken_Create) where a default value is not set.
444	Conversion to a physical card failed	Indicates that the create card request was successful, but the conversion to a physical card failed. The created card will be a virtual card.
445	Payment token count exceeds limit	Returned when a create token request (Ws_PaymentToken_Create) tries to create more tokens than allowed in the GPS database.
447	Cannot change status to expired. Expiry should be a system driven change.	The card expiry status is driven by the expiry date set in the system and cannot be manually applied to the card using the status code of 54. See Status Codes.
450	Token limit exceeded	Request is over the maximum number of card records (currently 1000 records) that can be cleared of cardholder data in a single web service call when using the Remove Cardholder Data (*Ws_Remove_CardHolder_Data*) web service.
500	Function not allowed by Institution	BOTTOM LINE (AGENCY BANKING SOLUTION)
501	Invalid Status Code	BOTTOM LINE (AGENCY BANKING SOLUTION)
502	Token Not Found	BOTTOM LINE (AGENCY BANKING SOLUTION)
503	Account Closed	BOTTOM LINE (AGENCY BANKING SOLUTION)
504	Account status was not updated successfully	BOTTOM LINE (AGENCY BANKING SOLUTION)
505	Apply to Account was not updated successfully	BOTTOM LINE (AGENCY BANKING SOLUTION)

Code	Description	How is it used?
506	Bank Transaction does not exists.	BOTTOM LINE (AGENCY BANKING SOLUTION)
507	Payment failed sanctions check.	BOTTOM LINE (AGENCY BANKING SOLUTION)
508	Payment to an Institution defined as a deny-listed account.	BOTTOM LINE (AGENCY BANKING SOLUTION)
509	BankingIn not allowed at Institution level	BOTTOM LINE (AGENCY BANKING SOLUTION)
510	BankingOut not allowed at Institution level	BOTTOM LINE (AGENCY BANKING SOLUTION)
511	DirectDebitIn not allowed at Institution level	BOTTOM LINE (AGENCY BANKING SOLUTION)
512	DirectDebitOut not allowed at Institution level	BOTTOM LINE (AGENCY BANKING SOLUTION)
513	BankingIn not switched on.	BOTTOM LINE (AGENCY BANKING SOLUTION)
514	Account in “not open” status but account status is a priority. BankingIn switched off.	BOTTOM LINE (AGENCY BANKING SOLUTION)
515	BankingOut not switched on.	BOTTOM LINE (AGENCY BANKING SOLUTION)
516	Account in “not open” status but account status is a priority. BankingOut switched off.	BOTTOM LINE (AGENCY BANKING SOLUTION)
517	DirectDebitIn not switched on.	BOTTOM LINE (AGENCY BANKING SOLUTION)
518	Account in “not open” status but account status is a priority. DirectDebitIn switched off.	BOTTOM LINE (AGENCY BANKING SOLUTION)
519	DirectDebitOut not switched on.	BOTTOM LINE (AGENCY BANKING SOLUTION)
520	Account in “not open” status but account status is a priority. DirectDebitOut switched off.	BOTTOM LINE (AGENCY BANKING SOLUTION)
521	Attempt to change account to disallowed status	BOTTOM LINE (AGENCY BANKING SOLUTION)
522	Amount to transfer must be a positive amount	BOTTOM LINE (AGENCY BANKING SOLUTION)
523	Sortcode cannot be empty	BOTTOM LINE (AGENCY BANKING SOLUTION)
524	Account number cannot be empty	BOTTOM LINE (AGENCY BANKING SOLUTION)
525	No available bank account numbers. Contact GPS	BOTTOM LINE (AGENCY BANKING SOLUTION)
526	Error creating bank account with required features	BOTTOM LINE (AGENCY BANKING SOLUTION)
527	Banking not allowed for this product	BOTTOM LINE (AGENCY BANKING SOLUTION)
528	No account associated with this token	BOTTOM LINE (AGENCY BANKING SOLUTION)
529	Payment from an Institution defined deny-listed account.	BOTTOM LINE (AGENCY BANKING SOLUTION)
530	Inbound processing payment code not allowed by Institution	BOTTOM LINE (AGENCY BANKING SOLUTION)
531	Inbound payment has error code. Processing not allowed by Institution	BOTTOM LINE (AGENCY BANKING SOLUTION)
532	Reversal not present	BOTTOM LINE (AGENCY BANKING SOLUTION)
533	Generic DDA Agency error	BOTTOM LINE (AGENCY BANKING SOLUTION)
534	Unknown DDA account number	BOTTOM LINE (AGENCY BANKING SOLUTION)
535	Direct debit was not cancelled	BOTTOM LINE (AGENCY BANKING SOLUTION)
536	BankingIn not allowed at Issuer level	BOTTOM LINE (AGENCY BANKING SOLUTION)
537	BankingOut not allowed at Issuer level	BOTTOM LINE (AGENCY BANKING SOLUTION)
538	DirectDebitIn not allowed at Issuer level	BOTTOM LINE (AGENCY BANKING SOLUTION)
539	DirectDebitOut not allowed at Issuer level	BOTTOM LINE (AGENCY BANKING SOLUTION)
540	Bottomline C series API not configured	BOTTOM LINE (AGENCY BANKING SOLUTION)
541	Combination of banking features not allowed	BOTTOM LINE (AGENCY BANKING SOLUTION)

Code	Description	How is it used?
542	DDA vales not configured	BOTTOM LINE (AGENCY BANKING SOLUTION)
543	Balance Sequence External Host is missing	Indicates the supplied parameter was an invalid value.
544	Invalid EHI Mode	Indicates the EHI mode of the Product is not valid for the operation.
545	Balance Sequence number is higner that the one inputted	Indicates the supplied parameter was an invalid value.
546	No direct debit found	BOTTOM LINE (AGENCY BANKING SOLUTION)
547	Issue connecting to Bottomline V Series	BOTTOM LINE (AGENCY BANKING SOLUTION)
548	Cannot close account with balance	BOTTOM LINE (AGENCY BANKING SOLUTION)
549	BACS payment cancelled by User	BOTTOM LINE (AGENCY BANKING SOLUTION)
550	BACS Error Code Q in file	BOTTOM LINE (AGENCY BANKING SOLUTION)
551	Peer to Peer transfer failed	BOTTOM LINE (AGENCY BANKING SOLUTION)
552	Peer to Peer reversal failed	BOTTOM LINE (AGENCY BANKING SOLUTION)
553	Peer to Peer not allowed between different PM	BOTTOM LINE (AGENCY BANKING SOLUTION)
554	Invalid character in reference field	BOTTOM LINE (AGENCY BANKING SOLUTION)
555	‘Banking transaction already processed	BOTTOM LINE (AGENCY BANKING SOLUTION)
556	Expected spend cannot be 0	Modulr (Agency Banking Service)
557	Must have at least 1 associate for the account	Modulr (Agency Banking Service)
558	Document must include a filename	Modulr (Agency Banking Service)
559	Document must have a filepath	Modulr (Agency Banking Service)
560	Document must have an uploaded date	Modulr (Agency Banking Service)
561	Associate must have an email	Modulr (Agency Banking Service)
562	Associate must have a first name	Modulr (Agency Banking Service)
563	Associate must have a last name	Modulr (Agency Banking Service)
564	Associate must have a phone number	Modulr (Agency Banking Service)
565	Associate phone number is not a recognised number	Modulr (Agency Banking Service)
566	Address line 1 is empty	Modulr (Agency Banking Service)
567	Address town is empty	Modulr (Agency Banking Service)
568	Address postcode is empty	Modulr (Agency Banking Service)
569	Address has invalid country code	Modulr (Agency Banking Service)
570	Product is not a Modulr product. Cannot create a customer	Modulr (Agency Banking Service)
571	Customer ID is not associated with this product	Modulr (Agency Banking Service)
572	Fauiled to save Modulr bank details	Modulr (Agency Banking Service)
573	Destination information provided with WEBHOOK call. Not needed	Modulr (Agency Banking Service)
574	No emails supplied when specifying EMAIL	Modulr (Agency Banking Service)
576	Passback Modurl Error	Modulr (Agency Banking Service)
577	Notfication already exists	Modulr (Agency Banking Service)
581	Modulr Payment unsuccessful	Modulr (Agency Banking Service)
583	IBAN is not valid	When the beneficiary IBAN is not provided in the request for a SEPA outbound payment (Modulr

Code	Description	How is it used?
		Agency Banking Service).
584	SEPAOut not allowed at Issuer level	When SEPAOut settings are not enabled at Issuer level (Modulr Agency Banking Service).
585	SEPAOut not allowed at Institution level	When SEPAOut settings not enabled at Institution level (Modulr Agency Banking Service).
588	Currency not supported	When any currency other than EUR is used for making SEPA Outbound payment. Only EUR currency is supported in SEPA (Modulr Agency Banking Service).
589	SEPAIn not allowed at Issuer level	When SEPAIn settings are not enabled at Issuer level (Modulr Agency Banking Service).
590	SEPAIn not allowed at Institution level	When SEPAIn settings are not enabled at Institution level (Modulr Agency Banking Service).
593	Modulr not enabled for this product. Please contact GPS support	When making a SEPA Outbound payment using a product which is not enabled for the Modulr Agency Banking Service).
594	KBA answer not provided	The 3D Secure *Add* or *Update* failed because the Type chosen is *KBA*, but KBA_Answer is not provided.
595	KBA question ID does not exist	The 3D Secure *Add* or *Update* failed because the Type chosen is *KBA*, but the KBA Value provided (question ID) does not exist.
596	Some conditions have not been met to remove cardholder data	The following conditions must be met before cardholder data can be deleted: • The number of years since the card was created must be greater than 6 years. • The actual or blocked amount on the card must be zero. • The card must be in the status of *Destroyed* or *Expired* card and the card must not be linked to an eWallet account.
599	Credential and token do not match	The 3D Secure Add/Update/Delete failed because the provided credentials do not belong to the provided public token. For an Update request for a KBA credential, this error is returned if the <KBA_AnswerOldValue> provided does not match the existing KBA credential value.
600	Invalid AuthCalendarGroup	Indicates the supplied value could not be found.
601	Invalid Product Code	Indicates supplied product code is invalid.
602	Invalid Scheduler Type	Indicates supplied scheduler type is invalid.
603	Quantity exceed the max limit	Quantity exceed the max limit.
604	Invalid Event ID	Indicates supplied event ID is invalid.
605	MVC token is missing or invalid	Indicates MVC token is missing or invalid.
606	Product of MVC token and destination token are not from same	Indicates MVC token and destination token do not belong to same product.
607	Source token is not MVC	Indicates source token is not MVC.
608	ClientID value is not present in the request	Indicates clientID is not present in the request.
609	Invalid FeeWaiver	Indicates FeeWaiver is invalid.
610	Partial fee is taken, remaining amount is stored for later	Partial fee is taken, remaining amount is stored for

Code	Description	How is it used?
		later.
611	No fee is taken, whole amount is stored for later	No fee is taken, whole amount is stored for later.
612	The sum of available balance and loaded value exceeds the maximum limit of balance amount.	The sum of available balance and loaded value exceeds the maximum limit of balance amount.
613	Invalid WSID specified in the request	Indicates supplied WSID is invalid.
614	Invalid Deny List	Indicates the supplied value could not be found.
615	Invalid Allow List	Indicates the supplied parameter value was not correct.
621	SFTP Is missing	SendCardFiles:SFTP Missing.
622	Invalid SMSBalance	Indicates the supplied parameter value was not correct.
623	Invalid load token, deny	Indicates the supplied parameter value was not correct.
624	Invalid Auth Type	Indicates the supplied parameter value was not correct.
625	Invalid ActMethod	Indicates the supplied parameter value was not correct.
626	SMS/Email subject cannot be blank.	Indicates the configured value was empty.
627	SMS/Email body cannot be blank.	Indicates the configured value was empty.
628	Token already exist in the table	3D Secure
629	Token is not configured to use the 3D secure web service	3D Secure
630	Token details set for delete.	3D Secure
631	LastModifiedType is missing	3D Secure
632	Invalid ListType	Sanction PEP
633	Invalid CheckLevel	Sanction PEP
634	Invalid Flag	Sanction PEP
635	Invalid Id	Sanction PEP
646	IssCode not configured for 3d secure	3D Secure
647	Invalid MatchItems	Sanction PEP
648	Missing DOB or Nationality	Sanction PEP
649	Update is Applicable only after processing of Insert (File is not yet processed)	Used when an attempt is made to update 3D Secure details before the initial details have been sent to the 3D Secure processing bureau.
650	Public token and new token have different billing currencies.	Primary and secondary cards should have same billing currency.
651	Invalid Sms_Required	Indicates the parameter value was invalid.
652	Invalid Sms_Content	Indicates the parameter value was invalid.
653	CSN is empty or badly formatted	Gemalto : CSN – given in custom1 field – is null, empty or badly formatted.
654	Card status cannot be changed, current status of the card is not reversible	Used when card is in an irreversible status: 43 or 83.
655	CSN is already associated with a card request in progress (i.e. a card request that has not yet reached a definitive status)	Gemalto : CSN – given in custom1 field – is already associated with a card request in progress (i.e. a card request that has not yet reached a definitive status)

Code	Description	How is it used?
656	Invalid DataSrc	Invalid data source
657	Authentication code is null, empty or badly formatted	Gemalto : Authentication code – given in custom2 field – is null, empty or badly formatted.
658	ExtAPICardID is missed in the request	Indicates the parameter value was missing.
659	Invalid load source is used in the request.	Please use load source Primary card (68) to transfer fund from primary to secondary and vice versa.
660	Invalid passcode (AccCode), it should be 6 digit number.	Leading zero is acceptable.
662	LockMode is invalid or missing	Indicates the parameter value was missing or an invalid value.
663	Invalid DOB	Indicates the parameter value was missing or an invalid value.
664	Invalid Fee, it should be decimal/integer	Indicates the parameter value was an invalid value.
665	Invalid ProductID	Indicates the parameter value was missing or an invalid value.
666	ProductID not belongs to the client	Indicates the parameter value was an invalid value for the PAN/Token supplied.
667	Forbidden load source(LoadSrc), this program manager has no right to use the selected load source.	Indicates the parameter value was an invalid value.
668	RSA – Invalid NamePrefix	Up to 120 characters allowed
669	RSA – Invalid NameSuffix	Up to 120 characters allowed
670	RSA – Invalid MothersMaidenName	Up to 120 characters allowed
671	RSA – Invalid CustomerID	Up to 120 characters allowed
672	RSA – Invalid AddressLine1	Up to 120 characters allowed
673	RSA – Invalid AddressLine2	Up to 120 characters allowed
674	RSA – Invalid City	Up to 120 characters allowed
675	RSA – Invalid StateCode	Two digits
676	RSA – Invalid CountryCode	Two characters according to ISO 3166-1 alpha-2 standards.
677	RSA – Invalid CompanyName	Up to 120 characters allowed
678	RSA – Invalid Misc1	Up to 120 characters allowed
679	RSA – Invalid Misc2	Up to 120 characters allowed
680	RSA – Invalid Misc3	Up to 120 characters allowed
681	RSA – Invalid Misc4	Up to 120 characters allowed
682	RSA – Invalid Misc5	Up to 120 characters allowed
683	RSA – Invalid Misc6	Up to 120 characters allowed
684	RSA – Invalid Misc7	Up to 120 characters allowed
685	RSA – Invalid Misc8	Up to 120 characters allowed
686	RSA – Invalid Last4SSN	Four digit integer
687	RSA – Invalid PANExp	Four digit integer
688	RSA – Invalid FullSSN	Nine digits
689	RSA – Invalid Last6SSN	Six digits
690	RSA – Invalid HomePhone	Up to 50 digit integer

Code	Description	How is it used?
691	RSA – Invalid BusinessPhone	Up to 50 digit integer
692	RSA – Invalid AltPhone1	Up to 50 digit integer. Also known as Mobile phone number.
693	RSA – Invalid AltPhone2	Up to 50 digit integer
694	RSA – Invalid ZipCode	Five digits
695	RSA – Invalid DayOfBirth	Two digits
697	RSA – Invalid MonthOfBirth	Two digits
698	RSA – Invalid YearOfBirth	Two digits
699	RSA – Invalid CreditLimit	Nine digits
700	Invalid ISO language code	Indicates the parameter value was missing or an invalid value.
701	Invalid CreateType	Indicates the parameter value was missing or an invalid value.
702	Invalid Currency Buy Rate.	Must be non-negative
703	Invalid Currency Sell Rate.	Must be non-negative
704	Invalid Currency Mid Rate.	Must be non-negative
705	Invalid source currency code	Indicates the parameter value was missing or an invalid value.
706	Invalid destination currency code	Indicates the parameter value was missing or an invalid value.
707	Invalid FX Group ID	Indicates the parameter value was missing or an invalid value.
708	Invalid Card Design, its a MutliFX product	Indicates the parameter value was missing or an invalid value.
709	Invalid currency code in MutliFXCurrencies	Indicates the parameter value was missing or an invalid value.
710	This Card Design does not support MultiFX	Indicates the parameter value was an invalid value.
711	This Card Design does not support External Authorisation	Indicates the parameter value was an invalid value for the operation.
712	Invalid Filter	Indicates the parameter value was missing or an invalid value.
713	Invalid Group Type	Indicates the parameter value was an invalid value.
714	Invalid load source	Indicates the parameter value was an invalid value.
715	invalid load fund type	Indicates the parameter value was an invalid value.
716	Invalid Linkage Group	Indicates the parameter value was an invalid value.
717	The specified PrimaryToken is not a primary card.	Secondary cards cannot be chosen as the Primary Card of another card.
718	Invalid PIN	PIN should be numeric and contain 4-12 digits.
719	Duplicate ExternalRef	Gemalto : requestUID value already exists for a card that is currently in production, or already produced.
720	Invalid TerminalID	Gemalto : satelliteUID value doesn’t exists in Dexxis I2 (Central Base can’t retrieve any Satellite with this ID).
721	Invalid ProductRef	Gemalto : cardTypeUID value doesn’t exists in Dexxis I2 (Central Base can’t retrieve any card type with this ID).

Code	Description	How is it used?
722	ExternalRef is empty	Gemalto : Null or empty string, or default value for parameter requestUID.
723	TerminalID is empty	Gemalto : Null or empty string for parameter satelliteUID.
724	ProductRef is empty	Gemalto : Null or empty string for parameter cardTypeUID.
725	CardName is empty	Gemalto : Null or empty string for parameter cardHolderName.
726	Some graphical data are empty	Gemalto : Null or empty array, or wrong size for parameter cardGraphicalData.
727	Some magnetic data are empty	Gemalto : Null or empty array, or wrong size for parameter cardMagneticalData.
728	Some carrier data are empty	Gemalto : Null or empty array or wrong size for parameter cardCarrierData.
729	Electric data is empty	Gemalto : Null or empty string for parameter cardElectricalData.
730	Illegal character in ExternalRef	Gemalto : requestUID contains characters that are not compatible with allowed charset/requestUID contains characters that are not alphanumerical.
731	Illegal character in TerminalID	Gemalto : satelliteUID contains characters that are not compatible with allowed charset/satelliteUID contains characters that are not alphanumerical.
732	Illegal character in ProductRef	Gemalto : cardTypeUID contains characters that are not compatible with allowed charset/cardTypeUID contains characters that are not alphanumerical.
733	Illegal character in graphical data	Gemalto : cardGraphicalData contains characters that are not compatible with allowed charset.
734	Illegal character in magnetic data	Gemalto : cardMagneticalData contains characters that are not compatible with allowed charset.
735	Illegal character in carrier data	Gemalto : cardCarrierData contains characters that are not compatible with allowed charset.
736	Grapical data type is empty or size is incorrect	Gemalto : Null or empty array, or wrong size for parameter cardGraphicalDataType.
737	Unknown graphical data type	Gemalto : cardGraphicalDataType contains at least one unknown graphical data type.
738	Size of graphical data and graphical data type aren’t identical	Gemalto : cardGraphicalDataType doesn’t contain the same number of values than cardGraphicalData.
739	Graphical data type doesn’t specified	Gemalto : At least one cardGraphicalData doesn’t have a cardGraphicalDataType specified.
740	Illegal character in electric data	Gemalto : cardElectricalData contains characters that are not compatible with allowed charset.
741	Custom data 1 is empty	Gemalto : Null or empty string, or default value for parameter cardRequestCustomData1.
742	Illegal character in custom data 1	Gemalto : cardRequestCustomData1 contains characters that are not compatible with allowed charset.
743	Custom data 2 is empty	Gemalto : Null or empty string, or default value for parameter cardRequestCustomData1.
744	Illegal character in custom data 2	Gemalto : cardRequestCustomData1 contains

Code	Description	How is it used?
		characters that are not compatible with allowed charset.
745	Custom data 3 is empty	Gemalto : Null or empty string, or default value for parameter cardRequestCustomData1.
746	Illegal character in custom data 3	Gemalto : cardRequestCustomData1 contains characters that are not compatible with allowed charset.
747	Custom data 4 is empty	Gemalto : Null or empty string, or default value for parameter cardRequestCustomData1.
748	Illegal character in custom data 4	Gemalto : cardRequestCustomData1 contains characters that are not compatible with allowed charset.
749	Custom data 5 is empty	Gemalto : Null or empty string, or default value for parameter cardRequestCustomData1.
750	Illegal character in custom data 5	Gemalto : cardRequestCustomData1 contains characters that are not compatible with allowed charset.
751	Illegal character in custom map file	Gemalto : cardRequestCustomMapFile contains characters that are not compatible with allowed encoding.
752	Incorrect custom map file XML format	Gemalto : XML file(s) contained into cardRequestCustomMapFile archive doesn’t have the required XML format.
753	Empty custom map file MD5 hash	Gemalto : Null or empty string for parameter cardProductionCustomMapFileMd5Hash.
754	Illegal character in custom map file MD5 hash	Gemalto : cardRequestCustomMapFileMd5Hash contains characters that are not compatible with allowed encoding. Hash result must be base64 encoded.
755	Comparison failed	Gemalto : cardRequestCustomMapFile archive transmission failure: MD5 hash comparison failed.
756	Unpack failed	Gemalto : cardRequestCustomMapFile archive can’t be unpacked or files can’t be retrieved from it. Probably an archive format error.
757	Map file data is not compactable with encoding	Gemalto : XML file(s) contained into cardRequestCustomMapFile archive contains at least one value that is not compatible with allowed encoding.
758	Invalid PIN Block	Gemalto : cipheredPin must contain 16 characters/cipheredPin parameter contains characters that are not compatible with allowed charset/cipheredPin parameter contains characters that are not allowed. cipheredPin must only be composed of digits or letters from A to F.
759	Invalid PIN Block format	Gemalto : cipheredPinFormat parameter is null or default values whereas it is mandatory since cipheredPin is set/cipheredPinFormat has not an attempted value (only ‘ISO0’ and ‘ISO2’ values are correct).
760	PIN block doesnot match PIN Block format	Gemalto : cipheredPin does not match given cipheredPinFormat.
761	PAN is empty	Gemalto : pan parameter is null or empty or default values whereas it is mandatory (given Ciphered PIN

Code	Description	How is it used?
		format is ISO0).
762	Invalid character in PAN	Gemalto : pan parameter contains characters that are not compatible with allowed charset/pan parameter contains characters that are not allowed. Pan must only be composed of digits.
763	Illegal character in PIN mailer data	Gemalto : At least one pinMailerData element contains characters that are not compatible with allowed charset.
764	Card request creation is forbidden	Gemalto : Card request creation is forbidden since standard Instant Issuance mode is deactivated on Central Base.
765	PIN can not verified	Gemalto : cipheredPin cannot been verified since KMS server is unreachable.
766	PIN delivery mode is empty	Gemalto : Null, empty or default string for parameter PinDeliveryMode whereas Pin or pinMailerData are provided.
767	Unkonwn PIN delivery mode	Gemalto : Unknown value for parameter PinDeliveryMode. Only NONE, PIN_MAILER and PIN_SELECTION are allowed.
768	Illegal character in Pin delivery mode	Gemalto : PinDeliveryMode parameter contains characters that are not compatible with allowed charset.
769	PIN Block is empty, choosen PIN delivery mode required PIN Block	Gemalto : cipheredPin parameter is null, empty or default value whereas it MUST contain a value because the chosen pinDeliveryMode requires it.
770	Data preparation failed	Gemalto : Data preparation failed (synchronous DP call) or data preparation launch failed (asynchronous DP call).
771	System is busy	Gemalto : The system is busy and can’t accept any new request for the moment. Either too many concurrent requests have been sent, or too many requests are currently waiting for data preparation. The system refuses new requests to remain stable and to keep acceptable performances. Please try again later and check the system health.
772	Request not found	Gemalto : Card Request not fount in Gemalto system.
773	Invalid ExpiryDatePart	Indicates the parameter value was invalid.
774	Limit Group not assigned to the input secondary card	Indicates the parameter value is not correctly configured.
775	Load source limit setting not found in the secondary card	Indicates the parameter value is not correctly configured.
776	The given card is already replaced	Indicates the parameter value is in an invalid state for the requested operation.
777	Invalid func	Indicates the parameter value was invalid.
778	Invalid PIN Mailer	Indicates the parameter value was invalid.
779	Deny list is empty	Indicates the parameter value was empty and is required.
780	Allow List is empty	Indicates the parameter value was empty and is required.

Code	Description	How is it used?
781	CardAcceptorId is empty	Indicates the parameter value was empty and is required.
782	Invalid Action	Indicates the parameter value was invalid.
783	CardAcceptorID not found	Indicates the parameter value was not found.
784	The requested product is virtual but the request is for physical card generation	Indicates the CreateType parameter value was invalid for the specified Product.
785	The requested product is physical but the request is for virtual card generation	Indicates the CreateType parameter value was invalid for the specified Product.
786	Invalid e-mail address	Indicates the parameter value was in an invalid format.
787	e-mail address is missing	Indicates the parameter value was empty and is required.
788	Invalid MailOrSMS	Indicates the parameter value was invalid.
789	Cannot convert card, card is already physical	Indicates the card has already been converted.
790	The card is physical, only virtual can convert	Indicates the card is already physical.
791	Load is disabled, card is EA Type1	Indicates the Product is configured as External Auth Type 1 where the client holds the balance and therefore Load is an invalid operation.
792	Wrong or expired login/password, or disabled user	The credentials supplied were invalid.
793	Wrong or insufficient credentials	The credentials were not properly supplied.
794	Login parameter is null, empty string, or default value	The credentials were not properly supplied.
795	Login parameter contains characters that are not compatible with allowed charset	The credentials were not properly supplied.
796	Password parameter is null, empty string, or default value	The credentials were not properly supplied.
797	Password parameter contains characters that are not compatible with allowed charset	The credentials were not properly supplied.
798	Quantity entered is invalid, it should be numeric and greater than one	Indicates the parameter value was invalid format.
799	This card acceptor is already added to the deny list/allow list of the given scheme	Indicates the card acceptor is already added to the deny list/allow list of the given scheme.
800	WSID is missing in the request.	Parameter was not supplied but is required.
801	IssCode is missing.	Parameter was not supplied but is required.
802	TxnCode is missing	Parameter was not supplied but is required.
803	AuthType is missing	Parameter was not supplied but is required.
804	LocDate is missing	Parameter was not supplied but is required.
805	LocTime is missing	Parameter was not supplied but is required.
806	CurCode is missing in the request.	Parameter was not supplied but is required.
807	DebOrCred is missing in the request.	Parameter was not supplied but is required.
808	Description is missing in the request.	Parameter was not supplied but is required.
809	Transaction amount such as AmtAjustment, LoadValue, UnloadValue is missing in the request.	Parameter was not supplied but is required.
810	PAN, PublicToken or CardDesign is missing in the request.	Parameter was not supplied but is required.
811	DOB is missing in the request.	Parameter was not supplied but is required.
812	CVV is missing.	Parameter was not supplied but is required.
813	AccCode is missing or invalid.	Parameter was not supplied but is required.

Code	Description	How is it used?
814	ClientCode is missing when AuthType is 5	Parameter was not supplied but is required.
815	LastName is missing when AuthType is 6	Parameter was not supplied but is required.
816	Track2 is missing when AuthType is 7	Track2 is mandatory when ActMethod is 4 or AuthMethod is 7 or when both PAN and PubToken are not provided.
817	SecId is missing when AuthType is 8.	Parameter was not supplied but is required.
818	SecVal is missing when SecValPos is non-zero.	Parameter was not supplied but is required.
819	ActMethod is missing in the request.	Parameter was not supplied but is required.
820	City or Postcode is missing in the request.	Parameter was not supplied but is required.
821	Country is missing	Parameter was not supplied but is required.
822	FirstName is missing in the request.	Parameter was not supplied but is required.
823	AccNo is missing in the request.	Parameter was not supplied but is required.
824	ExpDate is missing in the request.	Parameter was not supplied but is required.
825	StatCode or NewStatCode is missing or invalid in the request.	Parameter was not supplied but is required.
826	OrgItemId is missing in the request.	Parameter was not supplied but is required.
827	LoadFee is in incorrect format.	Parameter was supplied but is in an invalid format.
828	SecValPos in incorrect format.	Parameter was supplied but is in an invalid format.
829	SvcSrc is missing in the request.	Parameter was not supplied but is required.
830	SvcTye is missing in the request.	Parameter was not supplied but is required.
831	Work city or Work Postcode is missing in the request.	Parameter was not supplied but is required.
832	Work country is missing	Parameter was not supplied but is required.
833	Dlvcity or DlvPostcode is missing in the request.	Parameter was not supplied but is required.
834	DlvCountry is missing.	Parameter was not supplied but is required.
835	DlvFirstName is missing in the request.	Parameter was not supplied but is required.
836	SysDate is missing.	Parameter was not supplied but is required.
837	TxnType is missing.	Parameter was not supplied but is required.
838	TermCode is missing	Parameter was not supplied but is required.
839	TerminalID is missing.	Parameter was not supplied but is required.
840	CrdAcptLoc is missing.	Parameter was not supplied but is required
841	MCC is missing.	Parameter was not supplied but is required
842	Poschp is missing.	Parameter was not supplied but is required
843	Poscdim is missing.	Parameter was not supplied but is required
844	Poscham is missing.	Parameter was not supplied but is required
845	Poscp is missing.	Parameter was not supplied but is required
846	ItemId is missing.	Parameter was not supplied but is required
847	TlogId is missing.	Parameter was not supplied but is required
848	BillConvRate is missing.	Parameter was not supplied but is required
849	MsgType is missing.	Parameter was not supplied but is required
850	Func is missing.	Parameter was not supplied but is required

Code	Description	How is it used?
851	Current Pin is missing	Parameter was not supplied but is required
852	New Pin is missing	Parameter was not supplied but is required
853	Confirm Pin is missing	Parameter was not supplied but is required
854	Key ref is missing.	Parameter was not supplied but is required
855	ItemSrc is missing.	Parameter was not supplied but is required
856	LoadFundType is missing.	Parameter was not supplied but is required
857	LoadSrc is missing.	Parameter was not supplied but is required
858	LoadFee is missing.	Parameter was not supplied but is required
859	LoadedBy is missing.	Parameter was not supplied but is required
860	Title is missing.	Parameter was not supplied but is required
861	Addrl1 is missing.	Parameter was not supplied but is required
862	Addrl2 is missing.	Parameter was not supplied but is required
863	Reason is missing.	Parameter was not supplied but is required
864	Invalid Limit group code.	Parameter was supplied but is invalid
865	Invalid MCC group code.	Parameter was supplied but is invalid
866	Invalid Usage group code.	Parameter was supplied but is invalid
867	ProcCode is missing in the request or invalid.	Parameter was either supplied but is invalid, or is missing and required
868	Duplicate WSID in the request, deny.	The WSID has already been used on a previous request. WSIDs should be unique.
869	Invalid Fee Group Code	Parameter was supplied but is invalid
870	Invalid Primary Token, deny	Parameter was supplied but is invalid
871	Balance transfer from primary card to seconday or vice vers, deny	Not in use
872	Source and destination card has same PAN, deny	Attempt to balance transfer to and from same card is invalid
873	CardSelector is missing or invalid.	Parameter was not supplied but is required, or is an invalid value
874	CardSelectorValue is missing or invalid.	Parameter was not supplied but is required, or is an invalid value
875	Fee structure is not set for the given process code.	No fee structure is configured for the process code supplied during an attempt to take generic fees
876	RegenType/Replace is empty or invalid.	Parameter was not supplied but is required, or is an invalid value
877	Invalid expiry date.	An attempt was made to update the logical expiry date to either a past date, or a date that is beyond the physical expiry date
878	Invalid character in Card Name.	Non - european characters are not allowed in Card Name
879	Invalid character in First Name.	If Card Name is empty then non – european characters are not allowed in First Name.
880	Invalid character in Last Name.	If Card Name is empty then non – european characters are not allowed in Last Name.
881	Invalid recurring/scheduled fee group code.	Parameter was supplied but is invalid
882	Invalid web service fee group code.	Parameter was supplied but is invalid

Code	Description	How is it used?
883	Invalid Card Manufacturer Code	Parameter was supplied but is invalid
884	Customer mobile phone number is not set for this card.	An attempt was made to send an SMS, but no mobile number is registered for this card
885	Address verification failed.	The supplied address did not match the stored address
886	License verification failed.	The supplied License details did not match the stored details
887	Passport verification failed.	The supplied Passport details did not match the stored details
888	License number is missing.	A required parameter was not supplied
889	Gender (sex) is missing.	A required parameter was not supplied
890	Passport number is missing.	A required parameter was not supplied
891	Surname is missing.	A required parameter was not supplied
892	Passport number check digit is missing.	A required parameter was not supplied
893	Invalid DebOrCred,	It should be 1(Credit) or -1(Debit).
894	Invalid DOB format	Format should be YYYY-MM-DD
895	Invalid Start Date	Format should be YYYY-MM-DD
896	Invalid EndDate	Format should be YYYY-MM-DD
897	Invalid amount	Amount should be non-negative and no more decimal places than the currency will allow.
898	Invalid BIN/Manufacturer combination	The selected card manufacturer is not associated with the programme scheme
899	Invalid Country/Delv_Country, it should be ISO numeric code.	Parameter was supplied in incorrect format
900	Restricted web method, this client is not allowed to use this method	Client is not configured to call this web service
902	Invalid Transaction	The selected transaction is not valid for this operation
903	Re-Enter Transaction	The selected transaction must be re-entered
904	Format error, deny	Generic format error condition eg used by Account Enquiry to indicate invalid format in ‘txnfilter’ value received in request or when the security details do not match with the selected authMethod
905	Aquirer not supported by switch	As required by Issuer
906	Cutover in process	As required by Issuer
907	Card issuer signed off	As required by Issuer
908	Transaction destination cannot be found for routing	As required by Issuer
909	System malfunction, deny	Generic ‘catch-all’ error condition
910	Card issuer signed off	As required by Issuer
911	Card issuer timed out	As required by Issuer
912	Card issuer unavailable	As required by Issuer
913	Duplicate transaction, deny	To indicate the received request is a duplicate of a previous request. In some calls the ID of the original request (that this request duplicates) may also be returned in the response.

Code	Description	How is it used?
914	Unable to trace original transaction, deny	Used to indicate that the item a Void transaction seeks to cancel cannot be found
915	Reconcilliation cutover or checkpoint error	As required by Issuer
916	MAC incorrect	As required by Issuer
917	MAC key sync error	As required by Issuer
918	No communication keys available for use	As required by Issuer
919	Encryption key sync error	As required by Issuer
920	Security error – authentication failed, deny	Failed to authenticate the cardholder
921	Security error – security answer not defined	Failed to authenticate cardholder because one or more of the security details have not been setup for the cardholder
922	Message number out of sequence	As required by Issuer
923	Request in progress	As required by Issuer
924	Invalid security code	As required by Issuer
925	Database error	As required by Issuer
928	Customer vendor format	As required by Issuer
932	Recurring data error	As required by Issuer
933	Update not allowed	As required by Issuer
934	RegisterDetails was of the incorrect format	RegisterDetails was either empty or not of the correct type
935	RegisterSMS was of the incorrect format	RegisterSMS was either empty or not of the correct type
936	DeRegister was of the incorrect format	DeRegister was either empty or not of the correct type
937	OverrideGPS was of the incorrect format	OverrideGPS was either empty or not of the correct type
938	ReIssueBoolean was of the incorrect format	ReIssueBoolean was either empty or not of the correct type
939	NewToken was incorrect format	NewToken must be either 0 (if not re-issueing) or avalid public token
940	Value in a Detail was empty	Must have a value withing the Detail class and not empty string
941	ENUM_3DS_Details Identity was not a valid type	ENUM_3DS_Details Identity was not a valid type. Please see appendix for valid values
942	DetailsStatus was not a valid type	DetailsStatus was not a valid type. Please see appendix for valid values
943	MobileNumber was an invalid type	MobileNumber must be a valid number. Length must be between 11 and 25 characters long
944	SMSStatus was not a valid type	SMSStatus was not a valid type. Please see appendix for valid values
945	ReIssueBoolean is True and NewToken = 0	A request to reissue the details to a new token was received but the NewToken value is 0. Set NewToken to a valid public token
946	NewToken is an invalid token	A NewToken value has been requested but the supplied token is not valid
947	ReIssue and register are set	A request has been received to both register and

Code	Description	How is it used?
		reregister a token. Only one or the other can be done
948		Reserved for RSA
949		Reserved for RSA
950		Reserved for RSA
951	Webservice call successful, but failed to send Network Message due to internal error (i.e. 0302 service call did not return)	As required by Issuer
952	Webservice call successful, but failed to send Network Message due to message error (i.e. 0302 response was error)	As required by Issuer
954	RSA – Invalid BranchNumber	Ten digits
955	RSA – Invalid DateOfBirth	Must be format YYYYMMDD. Failed to convert to a date
956	RSA – Invalid LastStatementDate	Must be format YYYYMMDD. Failed to convert to a date
957	RSA – Invalid RelationshipType	Must be one of the following primary, co-applicant, authorized)
958	RSA – Invalid CompanyTel	Fifty digits
959	RSA – Invalid EmbossedName	Up to 120 characters allowed
960	RSA – Invalid FirstName	Up to 120 characters allowed
961	RSA – Invalid MiddleName	Up to 120 characters allowed
962	RSA – Invalid LastName	Up to 120 characters allowed
953	Activation of Card successful, but updating MDES Card Mapping failed	As required by Issuer
996	Retired Web Service	Retired
997	Soap username is null or empty	SOAP authentication
998	Soap password is null or empty	SOAP authentication
999	Security error – SOAP authentication failed. Deny	Indicates the SOAP authentication user name or password is incorrect.

MVC Action Codes

The following action codes are relevant to a Master Virtual Card (MVC) .

Code	Description
000	Normal, approve.
100	Do not Honour, deny.
116	Insufficient funds, deny.
118	No card record, deny.
121	Amount limits exceeded or outside valid load range, deny.
123	Frequency limits exceeded, deny.
605	MVC token is missing or invalid.
606	Source (MVC) and destination (new) tokens aren't belonging to same scheme.
607	Source token is not MVC.
661	MVC token and new token have different billing currencies. MVC load doesn’t support inter currency fund transfer.

Code	Description
801	IssCode is missing.
806	CurCode is missing in the request.
810	PublicToken is missing in the request.
897	Invalid amount, amount should be non-negative.
909	System malfunction, deny.
997	Soap username is null or empty.
998	Soap password is null or empty.
999	Security error. SOAP authentication failed. Deny.

Transaction Codes

The following transaction codes are used in the <TxnCode> tag of a web service response.

Code	Description
0	Card Activation
1	Card Load
2	Status Change
3	Balance Enquiry
4	Customer Enquiry
5	Card Statement
6	Load Verification
7	Balance Transfer
8	Card Unload
9	Card Enquiry
10	Activate / Load
11	Card Unload / Status Change
12	Transaction Void
13	Cardholder Update
14	Cardholder Details Enquiry
15	Load Demand
16	Balance Adjustment
17	Extend Expiry
18	Manage PIN
19	External Approve
20	Card Reload

SMS Configuration Options

Below are options for configuring the SMS messages sent to your customers. Please contact your Implementation Manager to ask for these SMS options to be configured.

Description	Examples
Web Services that allow configurable SMS text to be sent	PIN Control, Load, Unload, Balance Enquiry, Status Change, Activation, Card Create, Regenerate, Card Create (Replacement option), Balance Adjustment, Updated Cardholder.
Example variables that are allowed in configurable messages	Cardholder Title Cardholder First Name Cardholder Surname Card Currency (.e.g GBP) Amount (Load/Adjustment/Unload etc..) Current Available Balance CVV Masked PAN Masked replacement PAN PIN Sender (scheme sender)
Languages allowed	Language is determined by checking the current value of the cardholder *Lang* setting. For details, see Create Card.

Status Codes

The following status codes can be used within the <NewStatCode> tag to set the status of a card. They are also returned in a response to a card status request.

Status Code	Description
00	All Good. Indicates that the card is good for use, but does not indicate whether it is active. **Tip**: A card must have its <IsLive> flag changed to 1 to be considered active. You cannot activate a card by changing its status to 00. To activate a card, use Ws_Activate.
01	Refer to card issuer DO NOT USE
02	Card not yet activated
04	Capture Card
05	Do not honour
14	Invalid card (if you receive this status, it indicates that this card does not exist on the GPS system and was used for a fraudulent transaction) NEVER SET A CARD TO THIS STATUS
41	Lost card Do not use if temporarily blocking a tokenised digital PAN (DPAN). We recommend you use status code G1 instead.
43	Stolen card This status is irreversible.
46	Closed Account
54	Expired card DO NOT USE
57	Transaction not permitted to cardholder
59	Suspected Fraud
62	Restricted card
63	Security violation
70	Cardholder to contact issuer
75	Allowable number of PIN tries exceeded
83	Card destroyed This status is irreversible.
98	Refund given to customer
99	Card voided
G1	A short-term block which temporarily blocks card usage for all card transactions (excluding Credits and Refunds) for a short period.
G2	Short-term full block (all transactions are blocked).
G3	Long-term block (excluding Credits and Refunds).
G4	Long-term full block (all transactions are blocked).

Notes

- Most of the statuses are reversible. All of them apart from 00 will prevent the card from being used over the Mastercard or VISA network.
- Do not use status 01 (refer to Card Issuer or 54 (expired card) as these are for GPS use only.
- Changing the status to 99 (card voided) or 98 (refund to customer) automatically generates a card balance adjustment down to 0.00.
- You should use the following status codes for blocks:

- Temporary Block: G1 or G2.

  Use when you want merchants to try again. Visa guidelines instruct merchants to attempt up to 15 retries over 30 days. A card block will block all non-credit, Balance enquiry and tokenisation transactions. Refunds and Credits will be permitted.
- Permanent Block: G3 or G4. Use when you don’t want merchants to try again. Visa expect that the card should not return to the '00 Approve' state at all, or at least not within 30 days.

Transaction Status

Refer to the table below for a list of transaction status values for the <StatusCode> field.

Type	Description
A	Accepted
C	Cleared
I	Declined
R	Removed
S	Settled
V	Reversed

See usage in: Card Statement, Card Statement (V2)

Payment Token Types

Refer to the table below for a list of transaction types.

Type	Description
C	Contactless Device PAN
CF	Card on File PAN
CL	Cloud-base payments PAN
P	Real PAN (i.e. a normal ISO form factor card)
SE	Secure Element PAN
U	Unknown
V	Virtual PAN (i.e. virtual card)
BW	Browser-accessible wallet

String Cleaning and Approved Characters

GPS cleans any strings before adding to the database, limiting characters to the ASCII range of 33 to 122. This is aimed at stopping any unexpected characters in the core data for Authorisation, Presentments and Transactions, and to ensure data can be reliably used by EHI, Reporting, Smart Client and other systems.

Note: These lists are subject to change over time as printing capabilities and customer requirements change. For details, check with your Implementation Manager.

Characters Removed from Input Fields

The following special characters are removed from input fields:

Field	Special Characters that will be removed
CardName	;:!?\<>~#%@{}|[]”
FirstName	;:!?\<>~#%@{}|[]”
LastName	;:!?\<>~#%@{}|[]”
EmbossLine4	;,\:!?<>~`#%^@(){}|’[]”
Addrl1	;:!?\<>~`#%^@{}|[]”
Addrl2	;:!?\<>~`#%^@{}|[]”
Addrl3	;:!?\<>~`#%^@{}|[]”
City	;:!?\<>~`#%^@(){}|&[]”
PostCode	;:!?\<>~`#%^@(){}|&[]”
Country	;:!?\<>~`#%^@(){}|&[]”
Delv_AddrL1	;:!?\<>~`#%^@{}|[]”
Delv_AddrL2	;:!?\<>~`#%^@{}|[]”
Delv_AddrL3	;:!?\<>~`#%^@{}|[]”
Delv_City	;:!?\<>~`#%^@(){}|&[]”
Delv_County	;:!?\<>~`#%^@(){}|&[]”
Delv_PostCode	;:!?\<>~`#%^@(){}|&[]”
Delv_Country	;:!?\<>~`#%^@(){}|&[]”
Delv_Code	;:!?\<>~`#%^@(){}|&[]”
Fulfil1	;,/:!?\<>~`#%^(){}|&’[]”
Fulfil2	;,/:!?\<>~`#%^(){}|&’[]”
ThermalLine1	;:!?\<>~`#%^@(){}|&[]”
ThermalLine2	;:!?\<>~`#%^@{}|&[]”
Title	;:!?\<>~`#%^@(){}|&[]”
ImageId	;:!?\<>~`#%^@(){}|&[]”
LogoFrontId	;:!?\<>~`#%^@(){}|&[]”
LogoBackId	;:!?\<>~`#%^@(){}|&[]”
Mobile	;,:!?\<>~`#%^@-=*_$??(){}|&’[]”
ExternalRef	;,.\/:!?<>~`#%^@(){}&’[]”
CustAccount	;,.\/:!?<>~`#%^@(){}&’[]”

Field	Special Characters that will be removed
Email	;,/:!?\<>~`#%^(){}|&'[]"
Url	<>&'"
Reason	;,.\/!?<>~`#%^@(){}|&'[]”
Other string fields	;:!?\<>~`#%^@(){}|&[]”

Card Manufacturer Approved Characters

When submitting the *CardName* and *EmbossName* parameters (or *FirstName* and *LastName* if *CardName* is empty), please note that the card manufacturer only accepts the following approved characters:

Manufacturer	Allowed Characters
TCT	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
AllPay	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^/`',()+
GNC	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^+@&-'/,
GEMALTO	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
Nitecrest	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.- ^'ßÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÑÒÓÔÕÖØŠÙÚÛÜŸÝŽĄĆČĎĘĹĽŁŃŇŐŔŚŞŢŤŰŹŻ
Exceet	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^&'
Futurecard	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
DZ	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
ABNote	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
TrueB	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
MTL	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
CPI	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^`'
Rosan Finance	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^'
GyD	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^/&`',()+
Morpho	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^'
ArrowEye	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^/&`',()+
Nagra ID	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^/&`',()+
Gemalto - DCT	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
Intaremit	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
Gemalto Poland	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ-^aAcCeElLnNÓóSsZzZz
Austria Card	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^'
TAG	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^”“‘`'
DigiSEq	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
GPS	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
Borica	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
Gemalto Czech Republic	ABCDEFGHIJKLMNOPQRSTUVWXYZÄÜÖ/+-:;,.-@§D1234567890
Oberthur	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^/`',()+
Gemalto	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789&/-‘.,

Manufacturer	Allowed Characters
Singapore	
IDEMIA	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^/`',()+
CPI Card Group	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz1234567890ÄÅÆÇÉÑÖÜàáâäåæçèéêëìíîïñòóôöùúûü!@#$% ^&*()_+-=/|[]<>?;:'"ÀÁÂÃëÈÊËÌÍÎÏÒÓÔÕÙÚÛãðõœ
Verisoft	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^
Gemalto Brazil	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
CPI Group (UK)	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789($£€.,!?)
AB Corp	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
Catalyst	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
Gemalto Singapore	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
Goldpac	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
Gemalto AU	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
AB Corp AU	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
AB CORP NZ	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
GyD UK	ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789-. ‘
EVRY	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'
TOPPAN	abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789äöüÄÖÜ.-^',&\/?'

Replacement of Diacritic Letters

In addition to restricting the characters allowed, GPS also automatically replaces common diacritic letters with Latin alphabet letters. This applies only to track data used for the manufacturer files.

Diacritic Letter	Classic Latin Alphabet Letter
Á	A
á	a
Ä	A
ä	a
À	A
à	a
Â	A
â	a
Ã	A
ã	a
Å	A
å	a
Ç	C
ç	c
É	E
é	e

Diacritic Letter	Classic Latin Alphabet Letter
È	E
è	e
Ê	E
ê	e
Ë	E
ë	e
Í	I
í	i
Î	I
î	i
Ï	I
ï	i
Ì	I
ì	i
Ñ	N
ñ	n
Ó	O
ó	o
Ô	O
ô	o
Ò	O
ò	o
Ö	O
ö	o
Õ	O
õ	o
Ú	U
ú	u
Û	U
û	u
Ü	U
ü	u
Ù	U
ù	u
Ÿ	Y
ÿ	y
Ý	Y
ý	y
ß	S

Diacritic Letter	Classic Latin Alphabet Letter
Æ	AE
æ	ae
Œ	OE
œ	oe
Č	C
č	c
Ď	D
ď	d
Ě	E
ě	e
Ĺ	L
Í	I
Ľ	L
ľ	l
Ň	N
ň	n
Ő	O
ő	o
Ř	R
ř	r
Š	S
š	s
Ť	T
ť	t
Ű	U
ű	u
Ů	U
ů	u
Ž	Z
ž	z
Ø	O
Ą	A
ą	a
Ć	C
ć	c
Ę	E
ę	e
Ł	L
ł	l

Diacritic Letter	Classic Latin Alphabet Letter
Ń	N
ń	n
Ø	O
ø	o
Ŕ	R
ŕ	r
Ś	S
ś	s
Ș	S
ș	s
Ț	T
ț	t
Ź	Z
ź	z
Ż	Z
ż	z

Character Support in Web Services Calls

Postcode Permitted Characters

You can use the following characters in the Postcode field:

- Arabic numerals "0" to "9"
- letters of the ISO basic Latin alphabet (A-Z, a-z)
- spaces
- hyphens(-).

Card Name Permitted Characters

You can use the following characters in the CardName field:

- abcdefghijklmnopqrstuvwxyz
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 0123456789
- Some non-english characters i.e. “äöüÄÖÜ”
- “/” (forward slash)
- “-“ (hyphen)
- “^” (caret)
- “.” (full stop)
- “ “ (space character)
- “’” (apostrophe)

Processing of Phone Numbers

GPS processes telephone numbers in web services as follows:

- Deletes all special characters, including spaces, left and right parenthesis (i.e. brackets), and hyphens “-“.
- Deletes all leading non-numeric characters except “+”. Non-leading non-numeric characters (e.g. “-“) are not removed.
- Depending on the country, the national (domestic/inter-regional within a country) dialling prefix (e.g. single zero for many countries such as the UK, France, Spain, Australia) is dropped and "+" and the IDD (International Direct Dialing) number is prefixed. For example:
    - London, UK: 020 7292 2400 is changed to +442072922400
    - Lyon, France: 04 72 12 34 56 78 is changed to +3347212345678
    - Kuala Lumpur, Malaysia: 03 2123 4567 is changed to +60321234567
    - Mobile number, Spain: 0612 345 678 is changed to +34612345678
    - Sydney, Australia: 02 7010 1111 is changed to +61270101111
- If there is a "+" prefix, GPS checks if the digits which follow match the IDD number of the specified country. If they don't match, nothing is done. If they do match, GPS checks if the digits which follow match the national dialling prefix (e.g. single zero for many countries such as UK, France, Spain, Australia). If they do match, the national dialling prefix is dropped. For example:
    - London, UK: +44 020 7292 2400 is changed to +442072922400
    - Lyon, France: +33 04 72 12 34 56 78 is changed to +3347212345678
    - Kuala Lumpur, Malaysia: +60 03 2123 4567 is changed to +60321234567
    - Mobile number, Spain: +34 0612 345 678 is changed to +34612345678
    - Sydney, Australia: +61 02 7010 1111 is changed to +61270101111
- If there is no leading "+" or national dialling prefix, the phone number is stored as it is.

Currency Codes

Currency codes are based on the ISO 4217 specification.

The currency exponent is used in all fields containing an amount. See Amounts and Currency Exponents.

Code	Number	Exponent	Currency
AED	784	2	United Arab Emirates dirham
AFN	971	2	Afghan afghani
ALL	008	2	Albanian lek
AMD	051	2	Armenian dram
ANG	532	2	Netherlands Antillean guilder
AOA	973	2	Angolan kwanza
ARS	032	2	Argentine peso
AUD	036	2	Australian dollar
AWG	533	2	Aruban florin
AZN	944	2	Azerbaijani manat
BAM	977	2	Bosnia and Herzegovina convertible mark
BBD	052	2	Barbados dollar
BDT	050	2	Bangladeshi taka
BGN	975	2	Bulgarian lev
BHD	048	3	Bahraini dinar
BIF	108	0	Burundian franc
BMD	060	2	Bermudian dollar
BND	096	2	Brunei dollar
BOB	068	2	Boliviano
BOV	984	2	Bolivian Mvdol
BRL	986	2	Brazilian real
BSD	044	2	Bahamian dollar
BTN	064	2	Bhutanese ngultrum
BWP	072	2	Botswana pula
BYN	933	2	Belarusian ruble (new)
BYR	974	2	Belarusian Ruble (old)
BZD	084	2	Belize dollar
CAD	124	2	Canadian dollar
CDF	976	2	Congolese franc
CHE	947	2	Swiss WIR Euro
CHF	756	2	Swiss franc
CHW	948	2	Swiss WIR Franc
CLF	990	4	Chile Unidad de Fomento
CLP	152	0	Chilean peso
CNH	157	2	Chinese Offshore Renminbi/Yuan

Code	Number	Exponent	Currency
CNY	156	2	Chinese Renminbi/Yuan
COP	170	2	Colombian peso
COU	970	2	Unidad de Valor Real (UVR)
CRC	188	2	Costa Rican colon
CUC	931	2	Cuban convertible peso
CUP	192	2	Cuban peso
CVE	132	0	Cape Verde escudo
CZK	203	2	Czech koruna
DJF	262	0	Djiboutian franc
DKK	208	2	Danish krone
DOP	214	2	Dominican peso
DZD	012	2	Algerian dinar
EGP	818	2	Egyptian pound
ERN	232	2	Eritrean nakfa
ETB	230	2	Ethiopian birr
EUR	978	2	Euro
FJD	242	2	Fiji dollar
FKP	238	2	Falkland Islands pound
GBP	826	2	Great Britain (UK) Pound Sterling
GEL	981	2	Georgian lari
GHS	936	2	Ghanaian cedi
GIP	292	2	Gibraltar pound
GMD	270	2	Gambian dalasi
GNF	324	0	Guinean franc
GTQ	320	2	Guatemalan quetzal
GYD	328	2	Guyanese dollar
HKD	344	2	Hong Kong dollar
HNL	340	2	Honduran lempira
HRK	191	2	Croatian kuna
HTG	332	2	Haitian gourde
HUF	348	2	Hungarian forint
IDR	360	2	Indonesian rupiah
ILS	376	2	Israeli new shekel
INR	356	2	Indian rupee
IQD	368	3	Iraqi dinar
IRR	364	2	Iranian rial
ISK	352	0	Icelandic króna
JMD	388	2	Jamaican dollar
JOD	400	3	Jordanian dinar

Code	Number	Exponent	Currency
JPY	392	0	Japanese yen
KES	404	2	Kenyan shilling
KGS	417	2	Kyrgyzstani som
KHR	116	2	Cambodian riel
KMF	174	0	Comoro franc
KPW	408	2	North Korean won
KRW	410	0	South Korean won
KWD	414	3	Kuwaiti dinar
KYD	136	2	Cayman Islands dollar
KZT	398	2	Kazakhstani tenge
LAK	418	2	Lao kip
LBP	422	2	Lebanese pound
LKR	144	2	Sri Lankan rupee
LRD	430	2	Liberian dollar
LSL	426	2	Lesotho loti
LYD	434	3	Libyan dinar
MAD	504	2	Moroccan dirham
MDL	498	2	Moldovan leu
MGA	969	2	Malagasy ariary
MKD	807	2	Macedonian denar
MMK	104	2	Myanmar kyat
MNT	496	2	Mongolian tögrög
MOP	446	2	Macanese pataca
MRO	478	2	Mauritanian ouguiya (old)
MRU	929	2	Mauritanian ouguiya (new)
MUR	480	2	Mauritian rupee
MVR	462	2	Maldivian rufiyaa
MWK	454	2	Malawian kwacha
MXN	484	2	Mexican peso
MXV	979	2	Mexican Unidad de Inversion (UDI)
MYR	458	2	Malaysian ringgit
MZN	943	2	Mozambican metical
NAD	516	2	Namibian dollar
NGN	566	2	Nigerian naira
NIO	558	2	Nicaraguan córdoba
NOK	578	2	Norwegian krone
NPR	524	2	Nepalese rupee
NZD	554	2	New Zealand dollar
OMR	512	3	Omani rial

Code	Number	Exponent	Currency
PAB	590	2	Panamanian balboa
PEN	604	2	Peruvian sol
PGK	598	2	Papua New Guinean kina
PHP	608	2	Philippine peso
PKR	586	2	Pakistani rupee
PLN	985	2	Polish zloty (new)
PYG	600	0	Paraguayan guaraní
QAR	634	2	Qatari riyal
RON	946	2	Romanian leu
RSD	941	2	Serbian dinar
RUB	643	2	Russian ruble (old)
RUR	810	2	Russian ruble
RWF	646	0	Rwandan franc
SAR	682	2	Saudi riyal
SBD	090	2	Solomon Islands dollar
SCR	690	2	Seychelles rupee
SDG	938	2	Sudanese pound
SEK	752	2	Swedish krona/kronor
SGD	702	2	Singapore dollar
SHP	654	2	Saint Helena pound
SLE	925	2	Sierra Leonean leone (new)
SLL	694	2	Sierra Leonean leone (old)
SOS	706	2	Somali shilling
SRD	968	2	Surinamese dollar
SSP	728	2	South Sudanese pound
STD	678	2	São Tomé and Príncipe dobra (old)
STN	930	2	São Tomé and Príncipe dobra (new)
SVC	222	2	Salvadoran colón
SYP	760	2	Syrian pound
SZL	748	2	Swazi lilangeni
THB	764	2	Thai baht
TJS	972	2	Tajikistani somoni
TMM	795	0	Turkmenistan manat (old)
TMT	934	2	Turkmenistan manat (new)
TND	788	3	Tunisian dinar
TOP	776	2	Tongan pa-anga
TRL	792	2	Turkish lira
TRY	949	2	Turkish lira
TTD	780	2	Trinidad and Tobago dollar

Code	Number	Exponent	Currency
TWD	901	2	New Taiwan dollar
TZS	834	2	Tanzanian shilling
UAH	980	2	Ukrainian hryvnia
UGX	800	0	Ugandan shilling
USD	840	2	United States dollar
USN	997	2	US Dollar (next day)
USS	998	2	US Dollar (same day)
UYI	940	0	Uruguay Peso en Unidades Indexadas
UYU	858	2	Uruguayan peso
UYW	927	4	Unidad previsional
UZS	860	2	Uzbekistan som
VEF	937	2	Venezuelan Bolivar Fuerte (old)
VES	928	2	Venezuelan bolívar soberano (new)
VND	704	0	Vietnamese dong
VUV	548	0	Vanuatu vatu
WST	882	2	Samoan tala
XAF	950	0	CFA franc BEAC
XAG	961	2	Silver (one troy ounce)
XAU	959	2	Gold (one troy ounce)
XBA	955	2	European Composite Unit (EURCO) (bond market unit)
XBB	956	2	European Monetary Unit (E.M.U.-6) (bond market unit)
XBC	957	2	European Unit of Account 9 (E.U.A.-9) (bond market unit)
XBD	958	2	European Unit of Account 17 (E.U.A.-17) (bond market unit)
XCD	951	2	East Caribbean dollar
XDR	960	2	Special drawing rights
XOF	952	0	CFA franc BCEAO
XPD	964	2	Palladium (one troy ounce)
XPF	953	0	CFP franc (franc Pacifique)
XPT	962	2	Platinum (one troy ounce)
XSU	994	2	SUCRE
XTS	963	2	Code reserved for testing purposes
XUA	965	2	ADB Unit of Account
XXX	999	2	No currency
YER	886	2	Yemeni rial
ZAR	710	2	South African rand
ZMK	894	2	Zambian kwacha (old)
ZMW	967	2	Zambian kwacha (new)
ZWD	716	2	Zimbabwean dollar
ZWL	932	2	Zimbabwean dollar A/10

Amounts and Currency Exponents

Web service fields containing an amount can include up to four decimal places, depending on the currency exponent (e.g., 10.99 for EUR which has a currency exponent of 2). Below are examples of fields containing amounts:

```
AmtTxn, AvlBal, BlkAmt, AmtUnLoad, StartBal, EndBal, AmtBill, AmtTxn, FixedFee, RateFee, FxPdg, MCCPdg,
Dom_Fee_Fixed, Dom_Fee_Rate, Non_Dom_Fee_Fixed, Non_Dom_Fee_Rate, Fx_Fee_Fixed, Fx_Fee_Rate, Other_Fee_Desc,
Other_Fee_Amt, FxPdg, MCCPdg, AvlBalance_GPS_STIP, CurBalance_GPS_STIP, FINAMT, BLKAMT, AMTAVL, Fee, WaivedoffAmount,
TotalAmount, WaivedoffAmount
LimitInfo fields (V1):
MaxAllowableBalance, DailyLoadLimit, AmountLoaded, AmountLeftToLoad, DailyPosLimit, POSUsage, ValueOfPOSLeft,
DailyCashLimit, CashWithdrawal, ValueOfCashLeft, DailyUnLoadLimit, AmountUnLoaded, AmountLeftToUnLoad
LimitInfo fields (V2):
MaxPerTransaction, MinPerTransaction, Limit, Usage
```

General FAQs

This section provides answers to frequently asked questions.

Transactions

What is the primary key or identifier for a transaction?

ItemId is the primary key or identifier for a transaction.

Tokenisation Services

Where can I find out more about the GPS tokenisation service?

For detailed information on setting up and integrating the GPS tokenisation service, see the Tokenisation Service Guide.

How can I send an activation code to the cardholder's phone number?

If you want to use the SMS activation code service to send an Activation Code Notification (ACN) to the cardholder, you must include the mobile phone number of the cardholder when creating the card: first use the Card Create web service to create the card and then use the Card Activate web service to activate the card via SMS.

How do I send a confirmation SMS to the cardholder upon successful token activation in Apple Pay?

GPS can configure your product so that your end customers receive an SMS notification after successfully activating their Apple Pay token. You must ensure that you provide the cardholder's mobile number when creating the card.

> **Note:** GPS will receive a Tokenization Complete Notification (TCN) from Apple Pay if the activation is successful. We do not receive notifications for unsuccesful activations.

How can I retrieve the DPAN?

You can use the ws_Payment_Token_Get web service to get the DPAN for a card. See Payment Token Get.

The DPAN is returned in the <Payment_Token > field as a masked value.

Do GPS customers need to be PCI compliant to support MDES/VDEP?

To support MDES/VDEP integration on Android Pay or Apple Pay, customers must either be PCI DSS Compliant or be using a third party wallet provider for their virtual card. Both Apple and Google mandate Push Provisioning, which requires handling the full PAN.

GPS customers do not need to be PCI compliant for wallets that do not mandate Push Provisioning.

- **OUTOFBAND** – GPS sends the authentication request to your systems, using the endpoint set up for your Programme. Your systems must handle the authentication. For details, refer to the 3D Secure Guide.

> **Note:** OUTOFBAND is currently not available.

Document History

Refer to the table for details of changes to this guide..

Version	Date	Description	Author
1.1	30/11/2022	Updated the Copyright Statement.	MW
1.0	04/01/2021	First version of the guide.	WS

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Global Processing ServicesLtd.

Support Email: ops24@globalprocessing.com

Support Phone: +442037409682

GPS Offices

UK Central Office	Singapore	Australia	Dubai, UAE
6th Floor, Victoria House	Republic Plaza	Stone & Chalk	EO 10, Ground Floor,
Bloomsbury Square	9 Raffles Place	Level 4, 11 York Street	Building 1
London	Singapore	Wynyard Green	Dubai Internet City
WC1B 4DA	048619	Sydney, NSW, 2000	Dubai, United Arab Emirates

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@globalprocessing.com.

1 Glossary

3

3D Secure

3D Secure (3-domain structure), also known as a payer authentication, is a security protocol that helps to prevent fraud in online credit and debit card transactions. This security feature is supported by Visa and Mastercard and is branded as ‘Verified by Visa’ and ‘Mastercard SecureCode’ respectively.

A

Access Code

Pass code or activation code which you supply to GPS. You can use the access code to authenticate user access to card services or to request a user to activate the card by entering their access code.

Address Verification Service (AVS)

An AVS check compares the billing address used in the transaction with the issuing bank’s address information on file for that cardholder. Depending on whether they match fully, partially, or not at all, the merchant can use that information in their decision on whether or not to accept or cancel the order. AVS is one of the most widely used fraud prevention tools in card-not-present transactions.

Auth Calendar Group

Controls the dates and times when authorisations on a card are allowed. You can use this option to control when the card can be used, for example, prevent usage on weekends or out of hours.

B

BIN

A Bank Identification Number, or BIN, refers to the initial sequence of 4 to 6 numbers on a credit card and used to identify the card’s issuing bank or other financial institution. The BIN is the lynch pin that ties an issuer to its cards and transactions.

C

Card Linkage Group

The Linkage Group set up in Smart Client controls various parameters related to linked cards; for details, check with your Implementation Manager.

Card Manufacturer

GPS has relationships with existing card manufacturers, who we can instruct to print your cards. We use Secure FTP (sFTP) to send the card manufacturer a generated bulk XML file containing card details. This is sent on a daily basis, or at a frequency that can be customised for your service. The card manufacturer prints the cards and sends to the cardholder. Any white label test cards are typically sent to GPS, the Program Manager and the Card Schemes.

Card Service Code

3 digit code on the magnetic strip of a card which indicates where it is valid for use.

Card Verification Value

The Card Verification Value (CVV) on a credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. Cardholder's are typically required to enter the CVV during any online or cardholder not present transactions. CVV numbers are also known as CSC numbers (Card Security Code), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to guess.

Cardinal 3D Secure

Cardinal Commerce provide an Access Control Server (ACS) that enables support for the 3D Secure cardholder authentication scheme. See: https://www.cardinalcommerce.com

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction.

Concurrent session

The number of sessions (concurrent requests) that can be processed by the GPS server at the same time. This figure may vary, depending on server load and performance, which affects the response time. For example, an average server response time of 0.05ms.

CVC2

The Card Verification Value (CVV) on a credit card or debit card is a 3 digit number on VISA, MasterCard and Discover branded credit and debit cards. Cardholder's are typically required to enter the CVV during any online or cardholder not present transactions. CVV numbers are also known as CSC numbers (Card Security Code), as well as CVV2 numbers, which are the same as CVV numbers, except that they have been generated by a 2nd generation process that makes them harder to guess.

D

DPAN

Device PAN. The PAN value set up on the cardholder’s device. This is not visible to the cardholder, but is the PAN used for the transactions as far as the merchant is concerned.

E

EEA
European Economic Area

EHI
External Host Interface (EHI) is a GPS facility that enables exchange of data between the GPS processing centre and external systems using online web services. All transaction data processed by GPS is transferred to the External Host side via EHI in real time. For certain types of transactions such as Authorisations, the External Host can participate in payment transaction authorisation.

EHI Operation Mode
For authorisation type of transactions, the External Host Interface (EHI) can operate in one of five modes: Mode 1 the External Host maintains card balances and participates in transaction authorisation by approving or declining the transaction. Mode 2 - GPS maintains balances and performs all types of the authorization, but the External Host can overrule in some circumstances. Mode 3 - read-only data feed from the GPS system to the Client's system. Mode 4 - External Host maintains Balance (with GPS stand-in). Mode 5 – Same as EHI Mode 4, but clearing transactions do not update the GPS stand-in balance.

Expiry breakages
When a card with a fixed validity period, such as a gift card, expires, the available funds on the card are charged as an expiry breakage fee. The actual money is shared between GPS and the Program Manager.

External Host Interface (EHI)
The External Host Interface provides a facility to enable exchange of data between GPS and external systems via our web services. All transaction data processed by GPS is transferred to the External Host side via EHI in real time. For certain types of transactions, such as Authorisations, the External Host can participate in payment transaction authorisation.

F

Fee Group
Group which controls the card transaction authorisation fees.

FPAN
Funding PAN. The true 16-digit PAN of the card, which Mastercard/Visa converts when authorisations come through to them from Acquirers on the DPAN.

FX Fee Group
Controls the rates for FX currency conversions if the purchase currency is different from the card's currency.

G

GPS Scheme
The name of the high-level product type set up in GPS, usually at a BIN level.

I

Issuer Code
GPS Issuer (Program Manager) code, assigned by GPS. Each Program Manager is assigned their own unique issuer code on the system.

IVR system
Interactive Voice Response System Typically a telephony-based system, where the user calls in and selects options via an automated voice prompt.

L

Limit Group
Velocity limit group which restricts the frequency and/or amount at which the card can be loaded or unloaded. You can view your current Limit Groups in Smart Client.

M

Master Virtual Cards (MVC)
A GPS virtual card that is restricted to loading and unloading to a physical card and cannot be used for e-commerce or in-store transactions. An MVC is used to reflect the value of the ‘actual’ money in the Issuer's bank account. An MVC guarantees that the load is limited to the amount prefunded (i.e. loaded onto MVC) and gives the Programme Manager the ability to distribute funds immediately rather than having to wait for notification of each individual load into the Issuer Bank account.

Mastercard Digital Enablement Service
The MasterCard Digital Enablement Service (MDES) is a data interchange platform for generating and managing secure digital payment tokens.

MCC Group
Merchant Category Code (MCC) Group. The MCC is a four-digit number used by the Card Schemes to define the trading category of the merchant.

MDES
The MasterCard Digital Enablement Service (MDES) helps transform any connected device into a commerce device to make and receive payments. The MDES platform is used in iPhone 6, iPhone 6 Plus and Apple Watch to enable secure payments to take place for contactless and in-app

payments.

Merchant Category Codes (MCCs)

Merchant category codes (MCCs) are four-digit numbers that describe a merchant's primary business activities. MCCs are used by credit card issuers to identify the type of business in which a merchant is engaged.

MFX Card

Payment card which supports payment and settlement transactions in multiple currencies. The MFX card typically has a single PAN with multiple currency wallets linked.

O

Out of Band (OOB) Authentication

OOB authentication is a type of two-factor authentication that requires a secondary verification method through a separate communication channel along with the typical ID and password. For example, the user may be asked to respond to an automatically-generated phone call, enter a code sent to their smartphone or provide biometric verification via voice or fingerprint.

P

Padding amount

An additional amount or fee charged on a transaction, typically used to hedge against FX currency fluctuations or mitigate risks of higher declines or chargebacks for certain merchant categories.

PAN

A payment card number (PAN), primary account number, or simply a card number, is the card identifier found on payment cards, such as credit cards and debit cards, as well as stored-value cards, gift cards and other similar cards.

PCI DSS Compliant

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle credit cards from the major card schemes. All Program Managers who handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security/

PGP

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Product Setup Form

The Product Setup Form is a spreadsheet that provides details of your GPS account setup. The details are used to configure your GPS account.

PRODUCT_REF

The predefined reference code associated with the card, which is included in the XML file sent to the card manufacturer. This field is called the <ProductRef> on ws_create_card and the <DesignRef> on ws_customer_enquiry and ws_customer_enquiry_v2

ProductMaster

Card product-level master record

Program

Logical grouping of your products set up in Smart Client. This is setup with whatever the customer (issuer or program manager) wants. Can be viewed in reports or via the web services API and may also be sent to the card manufacturer.

Program Manager

A Program Manager is a GPS client who manages their own card service program.

Project Initiation Document (PID)

The Project Initiation Document (PID) is put together at a start of a project. This document outlines the initial project requirements and parties involved.

Project Requirements Document (PRD)

The Project Requirements Document (PRD) provides full details of the requirements of your project. Project schedules and implementation are based on the details provided in this document.

Project Scoping Document (PSD)

The Project Scoping Document (PSD) defines the scope of the project, and is typically produced before the start of the project.

PSD2

PSD2 is an EU Directive which sets requirements for firms that provide payment services. It introduces a number of requirements around how firms treat their customers and handle their complaints, and the data they must report to the FCA.

R

Race condition

When two separate processes are reading and updating a value at the same time, then the latest process can overwrite the previous saved result.

RSA

Provider of identity and access management solutions. See: https://www.rsa.com/

S

SAFE
SAFE (System to Avoid Fraud Effectively) is a Mastercard initiative requiring card issuers to report all cardholder fraud claims. The data sent to Mastarcard is used to help identify and track fraudulent activity. See: https://globalrisk.mastercard.com/online_resource/system-to-avoid-fraud-effectively-safe-compliance-program/

Scheduled Fee Group
Controls whether a card is charged a recurring fee, such as a monthly platform fee.

SchemeMaster
Card scheme-level master record

SFTP
Secure File Transfer Protocol. File Transfer Protocol FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Smart Client
Smart Client is GPS's user interface for managing your account on the GPS Apex system. It is also called Smart Processor GPS. Smart Client is installed as a desktop application and requires a VPN connection to GPS systems in order to be able to access your account.

SOAP
SOAP (Simple Object Access Protocol) is a messaging protocol for exchanging structured information in the implementation of web services. It uses Extensible Markup Language (XML) for its message format and relies on application layer protocols such as HTTP for message negotiation and transmission. SOAP allows developers to invoke processes running on disparate operating systems (such as Windows, macOS, and Linux) to authenticate, authorise, and communicate using XML.

STIP
Stand-In Processing. Where GPS holds the card balance on behalf of a Program Manager, in some instances where the Program Manager is not available, we are able to provide an authorisation decision for a transaction on their behalf.

U

Usage Group
Group that controls where a card can be used. For example: POS or ATM.

V

VDE
Virtual Data Element, used for 3D Secure identification. Examples are memorable name, memorable place and memorable date.

VPN
Virtual Private Network. A secure, encrypted remote connection over the public internet to the private GPS network, designed to safeguard the security and integrity of the network. Users are set up to access defined GPS services via their VPN connection.

W

Web Service Fee Group
Controls the fees charges for web service usage. Different web services can have different fees associated with them.

WSDL
Web Service Definition Language (WSDL) is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. WSDL files are central to testing SOAP-based services. SoapUI uses WSDL files to generate test requests, assertions and mock services.