GP webpay API HTTP

Technical specification for developers

Version: 1.18

Global Payments Europe, s.r.o.

Created **08.06.2016**

Last update **5.3.2024**

Author	GPE Product
Manager	GPE Application Development
Approved by	
Version	1.18
Confidentiality	Confidential

Document history:

Version	Date	Author	Comments
0.1	08.06.2016	GPE Product	Initial document version – revision of the document GP_webpay_Seznameni_se_systemem_v2.1
0.2	13.06.2016	GPE Product	Corrections
1.0	17.06.2016	GPE Application Development	Document revision
1.1	17.01.2017	GPE Application Development	Card number pattern/token verification functionality
1.2	15.06.2017	GPE Application Development	Card verification functionality Card on file (COF) functionality: - new value for input parameter USERPARAM1 - new fields in response
1.3	19.09.2018	GPE Application Development	New value in fields „PAYMETHOD“ and „PAYMETHODS“ for GooglePay
1.4	17.10.2018	GPE Application Development	New value in field „DISABLEPAYMETHOD “ for GooglePay Highlight the POST method when sending the response back to the merchant
1.5	1.11.2018	GPE Application Development	New parameter “FASTTOKEN” (COF enhancement) New feature – usage “FASTPAYID” or “FASTTOKEN” for direct payment – new value in field “USERPARAM1”
1.6	17.1.2018	GPE Application Development	New return parameter „TOKENREGSTATUS“ (COF registration)
1.7	15.3.2019	GPE Application Development	New fields in “ADDINFO” parameter Moving “Signing messages” chapter to a separate document
1.8	10.10.2019	GPE Application Development	New return parameters: - ACRC - RRN - PAR - TRACEID
1.9	16.1.2020	GPE Application Development	ApplePay implementation - new value for preferred paymet method - new value for disabled paymet method - new value for enabled paymet method
1.10	3.7.2020	GPE Application Development	Alternative payment methods - new value for preferred paymet method
1.11	10.8.2020	GPE Application Development	New Annex Annex no. 4 – Mandatory PSD2 data from the point of view of card schemes Description enhancement for return parameter MD
1.12	26.1.2021	GPE Application Development	Modification of the name of elements “cardholderInfo” and “cardholderDetail”
1.13	19.8.2021	GPE Application Development	Addinfo mandatory fields refinement. Small fixes.
1.13.1.	4.11.2021	GPE Application Development	Specification of the number of characters of the MERORDERNUM field
1.14	5.11.2021	GPE Application Development	Adding the default PAR value New template of the ADDINFO input parameter Modified description of mandatory fields from PSD2 perspective Removing the Masterpass service Removing the “Platba z účtu” service
1.15	15.12.2021	GPE Application Development	New payment buttons - ClickToPay (Click2Pay) - APM GPE – Alternative payment methods – payment buttons Description change on field DESCRIPTION PRCODE: - 37, 39

			SRCODE: - 1012, 1013
1.16	14.2.2023	GPE Application Development	Removing the “DISABLEPAYMETHOD” field – can be covered by using the “PAYMETHODS” field Extension of the list of supported APM GPE methods New attachment “Annex 5 – List of values for the fields “PAYMETHOD” and “PAYMETHODS”
1.17	15.10.2023	GPE Application Development	Extension of the list of supported APM GPE methods Extension of the list of supported values “Annex 5 – List of values for the fields “PAYMETHOD” and “PAYMETHODS” Removing the “USERPARAM1” field in response – can be covered by using the “TOKEN” field New element ADDINFO.SUBMERCHANT.merchantCountryOfOrigin Updated list of the ApplePay devices
1.18	21.2.2024	GPE Application Development	New element ADDINFO.paymentGatewayData Modified description of mandatory fields from PSD2 perspective

Table of contents

1. Formula clause

This document including any possible annexes and links is intended solely for the needs of an e-shop service provider (hereinafter referred to as “Customer”).

Information included in this document (hereinafter referred to as "Information") are subject to intellectual property and copyright protection of the Global Payments Europe, s.r.o. (hereinafter referred to as "GPE") and are of a commercially confidential nature in accordance with the provisions of the section 504 of the Act No. 89/2012 Coll., Civil Code. The Customer is aware of the legal obligations in relation to the handling of Information.

Information or any part thereof may not be provided or in any way made available to third parties without the prior written consent of the GPE. At the same time, Information may not be used by the Customer for purposes other than for the purpose for which it serves. To avoid any doubts, without the prior written consent of the GPE, Information or any part thereof may be provided or in any way made available neither to companies providing payment processing services on the Internet.

The GPE to the extent permitted by applicable law retains all rights to this document and Information contained therein. Any reproduction, use, exposure, or other publication, or dissemination of Information or its part by methods known and as yet undiscovered without the prior written consent of the GPE is strictly prohibited. The GPE is not in any way responsible for any errors or omissions in Information. GPE reserves the right, without giving any reason, to amend or repeal any Information.

2. Introduction

Technical specification for developers “GP webpay API HTTP” aims at e-commerce developers of merchants (hereinafter referred to as the developer), who perform integration of the e-shop with the GP webpay payment gateway using the API HTTP.

Integration using the API WS is described in the technical specification for developers “GP webpay API WS”.

Important notice: it is the acquirer who enables individual payment methods and functionalities to the merchant. Information regarding ordering of the GP webpay payment gateway and contacts to all the acquirers are available on www.gpwebpay.cz.

3. Process of payment

3.1 Request

If the customer requires on-line payment, the merchant creates a request for creating a payment in his/her e-shop (hereinafter referred to as the request) and sends it to the GP webpay payment gateway interface API HTTP.

Request format for individual payment methods is described below.

Complete list and sequence of parameters of a request are given in the following table:

Parameter	Type	Length	Mandatory
MERCHANTNUMBER **field included in digest**	character	10	yes
OPERATION **field included in digest**	character	20	yes
ORDERNUMBER **field included in digest**	numeric	15	yes
AMOUNT **field included in digest**	numeric	15	yes
CURRENCY **field included in digest**	numeric	3	yes/no *if not given, default currency from the merchant’s or bank’s settings is used*
DEPOSITFLAG **field included in digest**	numeric	1	yes
MERORDERNUM **field included in digest**	numeric	30 (16)	no
URL **field included in digest**	character	300	yes
DESCRIPTION **field included in digest**	character	255	no
MD **field included in digest**	character	255	yes/no
USERPARAM1 **field included in digest**	character	255	yes/no *mandatory for registration payment of the functionality Recurring*

			payment, Card on file, Card on file 3D, otherwise not mandatory
VRCODE **field included in digest**	character	48	yes/no *mandatory for cardholder verification via AC*
FASTPAYID **field included in digest**	numeric	15	yes/no *mandatory if the Fastpay service is used*
PAYMETHOD **field included in digest**	character	255	no
PAYMETHODS **field included in digest**	character	255	no
EMAIL **field included in digest**	character	255	no
REFERENCENUMBER **field included in digest**	character	20	no
ADDINFO **field included in digest**	XML scheme	24000	no
PANPATTERN **pole zahrnuto v digest**	character	255	no
TOKEN **pole zahrnuto v digest**	character	64	no
FASTTOKEN **pole zahrnuto v digest**	character	64	yes/no *mandatory if the Fasttoken service is used*
DIGEST	character	2000	yes
LANG **field NOT included in digest**	character	2	no

GP webpay API HTTP accepts only those requests, for which it can be proved that the originator of the request is an authorized subject, i.e. merchant with whom the acquirer has signed a contract.

DIGEST parameter is used to prove the origin of the request. Its content is generated on the basis of:

- Data sent: it proves that the contents of individual parameters has not been changed on the way to the system
- Private key: it proves that the request comes from the given merchant

When the integration begins, the merchant generates his/her private key using the GP webpay Portal; the merchant stores this key securely and provides it to the developer for integration. In the course of this process, the merchant's public key is stored automatically on the GP webpay server and before receiving a request from the merchant, it will be used to control if the merchant has signed the request with his/her private key.

DIGEST parameter, contained in the transmitted requests, contains electronic digest of all the other fields of the request. The digest ensures integrity and undeniableness of the transmitted request.

The request must meet the following conditions:

- In case that Redirect is used, the request is sent to the API HTTP by the GET method, or by means of sending the form data from the cardholder's internet browser by the GET or POST methods
- Parameters of the request must be signed in a clear and undeniable way. The DIGEST is created from the sent data contents using the merchant's private key (see the Annex no. 1 – Signing messages)
- Request is sent to the URL address according to the used environment:
    1. Client test environment: https://test.3dsecure.gpwebpay.com/pgw/order.do
    2. Production environment: https://3dsecure.gpwebpay.com/pgw/order.do
- Data transmitted in HTTP parameters of the request are x-www-form-urlencoded according to definition RFC 1866 – Chapter 8.2.2 (for more details see http://www.w3.org/MarkUp/html-spec/)
- HTTP request is sent via secured HTTPS channel using the server certificate provided by the GPE

In application GP webpay Portal, there can be downloaded other sources for integration with the GP webpay payment gateway using the API HTTP (e.g. examples of generating a digest (PHP, Java, .NET)).

After receiving the request, the GP webpay payment gateway creates an object named ORDER (see Chapter 4. Statuses of payment) and redirects the customer's browser to the payment page for payment method selection.

3.2 Response

After making the payment, the GP webpay payment gateway sends the result of payment to the merchant. The result is resent via customer's browser. Redirect (the GET method) or automatic form (the POST method) is used. Used method depends on the response parameters setting and on the provided services (DCC, installments …). Merchant's system must be able to process both possible methods.

Response format for individual payment methods is described below.

All the responses from the GP webpay contain also the DIGEST fields, the content of which is generated:

- On the basis of data contained in the response
- And at the same time, on the basis of the GP webpay private key

When the integration begins, from the GP webpay Portal the merchant downloads the GPE public key, which serves to verify the content of the DIGEST field.

This way the merchant can verify that:

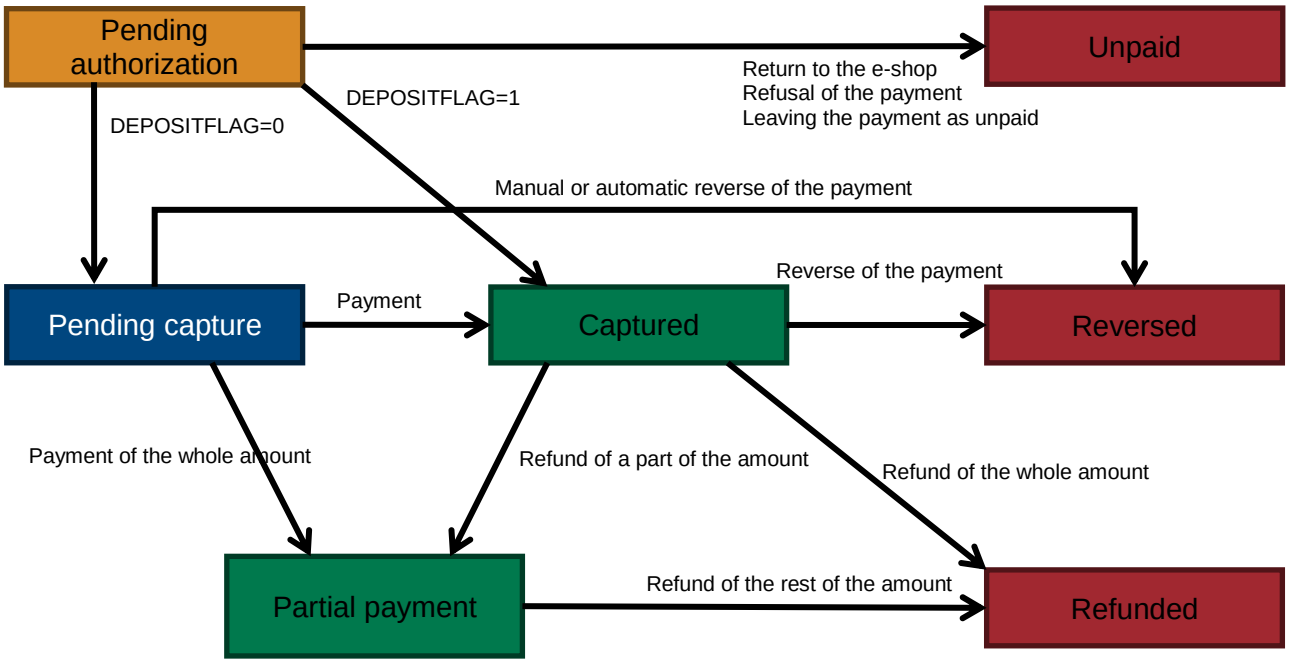
- The response really comes from the GP webpay
- The response has not been changed on the way.

Important notice: when processing the response, it is necessary to use only the parameters that are sent back by the GP webpay payment gateway.

4. Statuses of payment

After receiving the request, the GP webpay payment gateway creates an object named ORDER. Further options of payment management depend on the status, in which the request (ORDER) is, see the table and status diagram:

Status of payment	Description of payment status
Captured	Payment has been captured. Payment will be credited to the e-shop's account according to the contract with the bank for card acceptance on the Internet.
Unpaid	Payment has not been captured. The reason can be non-completion of the payment by the customer on the GP webpay payment gateway, customer's return from the GP webpay payment gateway to the e-shop, decline of payment in the systems of GPE, card association, and issuer, or technical problem.
Refunded	Payment has been refunded. Refund has been made by the e-shop by means of the GP webpay Portal (menu "Payments"), or using the Web Services.
Partial payment	Payment has been paid partially or refunded partially. Partial payment has been made by the e-shop by means of the GP webpay Portal (menu "Payments"), or using the Web Services.
Pending capture	Payment has been authorized by the issuer and the paid amount has been blocked on the customer's account. E-shop has the option to capture the amount from the customer's account later by means of the GP webpay Portal (menu "Payments"), or using the Web Services.
Pending authorization	Payment is processed. E-shop has created a payment request and the customer has the option to pay on the GP webpay payment gateway. Standard payments can be paid until expiry of the time interval for payment, PUSH payments can be paid until expiry of the payment link or exhaustion of attempts for payment.
Reversed	Payment has been reversed. The reverse has been made by the e-shop by means of the GP webpay Portal (menu "Payments"), or using the Web Services, or the payment gateway GP webpay after expiry of the time interval for blocking the amount on the customer's account by the issuer.



5. Card payment

5.1 Request format

Parameter	Type	Length	Mandatory	Note
MERCHANTNUMBER **field included in digest**	character	10	yes	A number assigned to each merchant.
OPERATION **field included in digest**	character	20	yes	**CREATE_ORDER value**
ORDERNUMBER **field included in digest**	numeric	15	yes	**Ordinal number of the order. Every request from a merchant has to contain a unique order number.**
AMOUNT **field included in digest**	numeric	15	yes	The amount in the smallest units of the relevant currency For CZK = in hellers, for EUR = in cents
CURRENCY **field included in digest**	numeric	3	yes/no *if not given, default currency from the merchant's or bank's settings is used*	Currency identifier according to ISO 4217 (see Addendum ISO 4217). **Multicurrency (using of various currencies)** depends on support provided by the respective bank. It is necessary to address your bank in this respect.
DEPOSITFLAG **field included in digest**	numeric	1	yes	Specifies if the order has to be paid for automatically. Values allowed: 0 = instant payment not required 1 = payment required
MERORDERNUM **field included in digest**	numeric	30 (16)	no	Order identification for the merchant. *If not specified, the ORDERNUMBER value is used*

				It is displayed in the bank statement. ***Each bank has its own solution/limit – Addendum no. 3 – Maximal length of merchantOrderNumber field*** **UP TO 16 DIGITS ARE CURRENTLY PROPAGATED TO THE PROVIDER'S SYSTEM. HOW MANY ARE SUBSEQUENTLY DISPLAYED ON THE STATEMENT IS SHOWN IN THE TABLE AT THE END OF THE DOCUMENT**
URL **field included in digest**	character	300	yes	Fully qualified merchant's URL. The request result is to be sent to this address. The result is resent via customer's browser. Redirect (the GET method) or automatic form (the POST method) is used. *(including protocol specification - e.g. https://)* For security reasons, certain forms of URL address can be blocked – e.g. using of parameters in the address. This check cannot be switched off and it is necessary to test a real form of the return address in the testing environment.
DESCRIPTION **field included in digest**	character	255	no	Description of the purchase. The field may contain only ASCII characters ranging from 0x20 to 0x7E.
MD **field included in digest**	character	255	yes/no	Any merchant's data returned to the merchant in the response in the unchanged form – only "whitespace" characters are removed from both sides. The field is used to satisfy various demands of the e-shops. The field may only contain ASCII characters ranging from 0x20 to 0x7E. If it is necessary to transmit any other data, BASE64 encoding must be used (see Addendum no. 1 – BASE64 encoding and decoding). The field must not contain any personal data. **The resulting length of the data must not exceed 255 B.**
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. If the parameter is sent but the device used does not support the required payment method, other payment methods are offered. Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields
PAYMETHODS **field included in digest**	character	255	no	List of allowed payment methods. Values are separated by comma ",". Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields
EMAIL **field included in digest**	character	255	no	Card holder's e-mail will be used for notification of the payment result and in the antifraud systems (FDS). The field must contain only **one** valid e-mail address.
REFERENCENUMBER **field included in digest**	character	20	no	Internal ID at the merchant's Supported ASCII characters: x20(space), x23(#), x24($), x2A-x3B(*+,-./0-9:;), x3D(=), x40-x5A(@A-Z), x5E(^), x5F(_), x61-x7A(a-z)
ADDINFO **field included in digest**	XML scheme	24000	no	Basket description, data for FDS, additional information about the customer…

				May optionally be used for display the basket in wallets. **We highly recommend sending requests to the payment gateway using the POST method. This removes the limit of data length in the address bar (GET method) and ensures preservation of the national characters coding in UTF-8 format.** **Another recommendation is not to use spacing and spaces/whitespaces between XML elements. Browsers usually do not work very correctly with it and interpret spacing differently. In most cases this ends with signature non-verification on the server.**
DIGEST	character	2000	yes	A check signature of the string generated as a concatenation of the fields in the order given in this table – Annex no. 1 – Signing messages *In case of the incorrect data signature the exception report is sent back to the Internet browser, which has sent this request.*
LANG **field NOT included in digest**	character	2	no	Value indicating automatic choice of language at the payment gateway. Abbreviation of one of the supported languages must be used – see the list at the payment gateway.

5.2 Response format

Parameter	Type	Length	Mandatory	Note
OPERATION **field included in digest**	character		yes	**CREATE_ORDER value**
ORDERNUMBER **field included in digest**	numeric	15	yes	Contents of the field from the request.
MERORDERNUM **field included in digest**	numeric	30	no	Contents of the field from the request, if included.
MD **field included in digest**	character	255	no	Contents of the field from the request, if included. If the provider uses an online notification component (GPE Integration Advice Switch), the ID value is added to the content of the MD field. Eg.: #ID=200323-S1APST31-000001299560 If the merchant has PayPal enabled and the payment is made through this channel, the PayPal ID value is added to the MD value. Eg.: #IDPP=2RN85480PL048943C
PRCODE **field included in digest**	numeric		yes	Primary code. For details, see “List of return codes”.
SRCODE **field included in digest**	numeric		yes	Secondary code. For details, see “List of return codes”.
RESULTTEXT **field included in digest**	character	255	no	A text description of the error identified by a combination of PRCODE and SRCODE. The contents are coded using the Windows Central European (Code Page 1250).
ADDINFO **field included in digest**	XML scheme		no	The field is filled in depending on settings of the input parameters for wallets and requested return information (payment card brand…). **If sending this field is requested (depends on data settings in the “ADDINFO” input parameter),**

				response will be sent by POST method. The reason is the size limit of data sent by the GET method (address barcode of the browser) and secure determination of character set of the response – UTF-8.
TOKEN **field included in digest**	character	64	no	Unique identifier of the payment card calculated by the GP webpay system
EXPIRY **field included in digest**	character	4	no	Expiry date of the used payment card in the YYMM format
ACSRES **field included in digest**	character	1	no	Authentication result of the cardholder in the 3D system Possible values: N = an attempt for authentication has not been made – some card associations do not support 3D authentication A = an attempt for authentication has been made, however the card does not participate in the 3D system or the bank does not support the system F = the cardholder is fully authenticated D = the card has not been authenticated successfully (declined) – wrong authentication data E = technical problem with cardholder's authentication
ACCODE **field included in digest**	character	6	no	Authorization code of the payment obtained from the authorization center The field must be approved by provider.
PANPATTERN **field included in digest**	character	20	no	Masked number of the payment card used in the 6{***}4 format
DAYTOCAPTURE **field included in digest**	character	8	no	The last day for capture request. Format: DDMMYYYY.
TOKENREGSTATUS **field included in digest**	character	10	no	Token registration status Possible values: SUCCESS – Token has been successfully registered EXISTOWNER – The card has already been registered and the token has been registered by the merchant requesting the registration EXISTOTHER – The card has already been registered and the token has been registered by another merchant in the group
ACRC **field included in digest**	character	1-2	no	The "Authorization return code" – a detailed indication of the authorization result. (the field must be approved by the provider)
RRN **field included in digest**	character	1-12	no	The Retrieval Reference Number data element contains a number assigned by the message GP webpay to uniquely identify a transaction. This number remains unchanged for all messages throughout the life of a transaction. (the field must be approved by the provider)
PAR **field included in digest**	character	1-29	no	The Payment Account Reference – unique value for the bank account of the cardholder (can be the same for more than one payment card). **For cards that do not yet have a PAR value, the default value of "V0010000000000000000000000000000" can be returned. This value does NOT point to any specific account.**

TRACEID **field included in digest**	character	1-15	no	TraceID returned by authorization system
DIGEST	character	2000	yes	A check signature of the string generated as a concatenation of all the fields sent in the given order – Annex no. 1 – Signing messages
DIGEST1	character	2000	yes	A check signature of the string generated as a concatenation of all the fields sent in the given order (without the DIGEST field) and on the top of that also the MERCHANTNUMBER field (the field is not sent, the merchant has to know it, the field is added to the end of the string). Security and unambiguity of the response is increased in this way. *Verification of the signature is identical to the DIGEST field.*

The merchant must work ONLY with fields that he/she RECEIVES, not with fields about which he/she "thinks" that should be received.

6. Card verification

"Verification" request without blocking money.

6.1 Request format

Parameter	Type	Length	Mandatory	Note
MERCHANTNUMBER **field included in digest**	character	10	yes	A number assigned to each merchant.
OPERATION **field included in digest**	character	20	yes	**CARD_VERIFICATION value**
ORDERNUMBER **field included in digest**	numeric	15	yes	**Ordinal number of the order. Every request from a merchant has to contain a unique order number.**
MERORDERNUM **field included in digest**	numeric	30 (16)	no	Order identification for the merchant. *If not specified, the ORDERNUMBER value is used* *It is displayed in the bank statement.* ***Each bank has its own solution/limit – Addendum no. 3 – Maximal length of merchantOrderNumber field*** **UP TO 16 DIGITS ARE CURRENTLY PROPAGATED TO THE PROVIDER'S SYSTEM. HOW MANY ARE SUBSEQUENTLY DISPLAYED ON THE STATEMENT IS SHOWN IN THE TABLE AT THE END OF THE DOCUMENT**
URL **field included in digest**	character	300	yes	Fully qualified merchant's URL. The request result is to be sent to this address. The result is resent via customer's browser. Redirect (the GET method) or automatic form (the POST method) is used. *(including protocol specification - e.g. https://)* For security reasons, certain forms of URL address can be blocked – e.g. using of parameters in the address. This check cannot be switched off and it is necessary to test a real form of the return address in the testing environment.

DESCRIPTION **field included in digest**	character	255	no	Description of the purchase. The field may contain only ASCII characters ranging from 0x20 to 0x7E.
MD **field included in digest**	character	255	no	Any merchant's data returned to the merchant in the response in the unchanged form – only "whitespace" characters are removed from both sides. The field is used to satisfy various demands of the e-shops. The field may only contain ASCII characters ranging from 0x20 to 0x7E. If it is necessary to transmit any other data, BASE64 encoding must be used (see Addendum no. 1 – BASE64 encoding and decoding). The field must not contain any personal data. **The resulting length of the data must not exceed 255 B.**
EMAIL **field included in digest**	character	255	no	Card holder's e-mail will be used for notification of the payment result and in the antifraud systems (FDS). The field must contain only **one** valid e-mail address. The field may contain any characters, but if e-mail address contains national characters, we recommend using see Addendum no. 1 – BASE64 encoding and decoding.
REFERENCENUMBER **field included in digest**	character	20	no	Internal ID at the merchant's Supported ASCII characters: x20(space), x23(#), x24($), x2A-x3B(*+,-./0-9:;), x3D(=), x40-x5A(@A-Z), x5E(^), x5F(_), x61-x7A(a-z)
ADDINFO **field included in digest**	XML scheme	24000	no	Basket description, data for FDS, additional information about the customer… May optionally be used for display the basket in wallets. **We highly recommend sending requests to the payment gateway using the POST method. This removes the limit of data length in the address bar (GET method) and ensures preservation of the national characters coding in UTF-8 format.** **Another recommendation is not to use spacing and spaces/whitespaces between XML elements. Browsers usually do not work very correctly with it and interpret spacing differently. In most cases this ends with signature non-verification on the server.**
DIGEST	character	2000	yes	A check signature of the string generated as a concatenation of the fields in the order given in this table – Annex no. 1 – Signing messages *In case of the incorrect data signature the exception report is sent back to the Internet browser, which has sent this request.*
LANG **field NOT included in digest**	character	2	no	Value indicating automatic choice of language at the payment gateway. Abbreviation of one of the supported languages must be used – see the list at the payment gateway.

6.2 Response format

Parameter	Type	Length	Mandatory	Note
OPERATION **field included in digest**	character		yes	**CARD_VERIFICATION value**
ORDERNUMBER **field included in digest**	numeric	15	yes	Contents of the field from the request.
MERORDERNUM **field included in digest**	numeric	30	no	Contents of the field from the request, if included.
MD **field included in digest**	character	255	no	Contents of the field from the request, if included.
PRCODE **field included in digest**	numeric		yes	Primary code. For details, see “List of return codes”.
SRCODE **field included in digest**	numeric		yes	Secondary code. For details, see “List of return codes”.
RESULTTEXT **field included in digest**	character	255	no	A text description of the error identified by a combination of PRCODE and SRCODE. The contents are coded using the Windows Central European (Code Page 1250).
ADDINFO **field included in digest**	XML scheme		no	The field is filled in depending on settings of the input parameters for wallets and requested return information (payment card brand…). **If sending this field is requested (depends on data settings in the “ADDINFO” input parameter), response will be sent by POST method. The reason is the size limit of data sent by the GET method (address barcode of the browser) and secure determination of character set of the response – UTF-8.**
TOKEN **field included in digest**	character	64	no	Unique identifier of the payment card calculated by the GP webpay system
EXPIRY **field included in digest**	character	4	no	Expiry date of the used payment card in the YYMM format
ACSRES **field included in digest**	character	1	no	Authentication result of the cardholder in the 3D system Possible values: N = an attempt for authentication has not been made – some card associations do not support 3D authentication A = an attempt for authentication has been made, however the card does not participate in the 3D system or the bank does not support the system F = the cardholder is fully authenticated D = the card has not been authenticated successfully (declined) – wrong authentication data E = technical problem with cardholder’s authentication
ACCODE **field included in digest**	character	6	no	Authorization code of the payment obtained from the authorization center (the field must be approved by the provider)
PANPATTERN **field included in digest**	character	20	no	Masked number of the payment card used in the 6{***}4 format
DAYTOCAPTURE	character	8	no	The last day for capture request.

field included in digest				Format: DDMMYYYY.
TOKENREGSTATUS **field included in digest**	character	10	no	Token registration status Possible values: SUCCESS – Token has been successfully registered EXISTOWNER – The card has already been registered and the token has been registered by the merchant requesting the registration EXISTOTHER – The card has already been registered and the token has been registered by another merchant in the group
ACRC **field included in digest**	character	1-2	no	The “Authorization return code” – a detailed indication of the authorization result. (the field must be approved by the provider)
RRN **field included in digest**	character	1-12	no	The Retrieval Reference Number data element contains a number assigned by the message GP webpay to uniquely identify a transaction. This number remains unchanged for all messages throughout the life of a transaction. (the field must be approved by the provider)
PAR **field included in digest**	character	1-29	no	The Payment Account Reference – unique value for the bank account of the cardholder (can be the same for more than one payment card). **For cards that do not yet have a PAR value, the default value of "V0010000000000000000000000000000" can be returned. This value does NOT point to any specific account.**
TRACEID **field included in digest**	character	1-15	no	TraceID returned by authorization system
DIGEST	character	2000	yes	A check signature of the string generated as a concatenation of all the fields sent in the given order – Annex no. 1 – Signing messages
DIGEST1	character	2000	yes	A check signature of the string generated as a concatenation of all the fields sent in the given order (without the DIGEST field) and on the top of that also the MERCHANTNUMBER field (the field is not sent, the merchant has to know it, the field is added to the end of the string). Security and unambiguity of the response is increased in this way. *Verification of the signature is identical to the DIGEST field.*

The merchant must work ONLY with fields that he/she RECEIVES, not with fields about which he/she “thinks” that should be received.

7. Payment using digital wallet

7.1 Google Pay

Google Pay is the Google system enabling the use of payment cards stored in the Google account to make payments on the Internet.

The payment method may not be available for all types of hardware and browsers. Before offering payment, the device is tested and after evaluation, the payment button is displayed or hidden.

In order to make a payment via Google Pay, the customer clicks the “G Pay” button and a page containing information for the customer is displayed. After pressing the “Pay” button, the customer logs in into his/her Google account and chooses which of the stored cards he/she wants to use to make the payment. The payment may require the 3D Secure security including cardholder authentication by the issuer.

Google Pay can be offered directly on the webpages of the e-shop by means of the “Google Pay” button. To integrate e-shop for this case of use, the “PAYMETHOD” parameter with value “GPAY” is used in the request. **If the parameter is sent but the device used does not support the required payment method, other payment methods are offered.**

Parameter	Type	Length	Mandatory	Note
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields **GPAY – GooglePay**

7.2 Apple Pay

Apple Pay is the Apple system enabling the use of payment cards stored in the Apple account to make payments on the Internet.

The payment method may not be available for all types of hardware and browsers. Before offering payment, the device is tested and after evaluation, the payment button is displayed or hidden.

Devices compatible with Apple Pay (https://support.apple.com/en-us/102896):

- compatible iPhone models:
  - iPhone models with Face ID
  - iPhone models with Touch ID, except iPhone 5s
- compatible iPad models:
  - iPad Pro, iPad Air, iPad, and iPad mini models with Touch ID or Face ID
- compatible Apple Watch models:
  - Apple Watch Series 1 and later
- compatible Mac models:
  - Mac models with Touch ID
  - Mac models introduced in 2012 or later with an Apple Pay-enabled iPhone or Apple Watch

- Mac computers with Apple silicon that are paired with a Magic Keyboard with Touch ID

In order to make a payment via Apple Pay, the customer clicks the “A Pay” button and a page containing information for the customer is displayed. After pressing the “Pay” button, the customer logs in into his/her Apple account and chooses which of the stored cards he/she wants to use to make the payment.

Apple Pay can be offered directly on the webpages of the e-shop by means of the “Apple Pay” button. To integrate e-shop for this case of use, the “PAYMETHOD” parameter with value “APAY” is used in the request. **If the parameter is sent but the device used does not support the required payment method, other payment methods are offered.**

Parameter	Type	Length	Mandatory	Note
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields **APAY – Apple Pay**

8. Payments with payment button

The following payment methods can be offered directly on the e-shop website via the button and using the parameter "PAYMETHOD" with the appropriate value. After being redirected to the payment gateway, the desired method is immediately offered. If the merchant does not have the selected method active or not available, the standard card payment is offered.

8.1 PLATBA 24 – direct contract with Česká spořitelna

PLATBA 24 can be offered directly on the webpages of the e-shop by means of the “PLATBA 24” button. To integrate e-shop for this case of use, the “PAYMETHOD” parameter with value “BTNCS” is used in the request:

Parameter	Type	Length	Mandatory	Note
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields **BTNCS – PLATBA 24 – payment button České spořitelny**

8.2 Alternative payment methods (APMs) – GP/PPRO provider (ongoing)

The methods will be phased out and replaced by a GPE provider.

The GP webpay system provides some other alternative payment methods.

The availability of methods is limited by their support on the part of the provider.

Available methods:

- SOFORT
- EPS
- PAYSAFECARD
- SEPADIRECTDEBIT
- KLARNA
- PAYPAL

Parameter	Type	Length	Mandatory	Note
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields **SOFORT** **EPS** **PAYSAFECARD** **SEPADIRECTDEBIT** **KLARNA** **PAYPAL**

8.3 Alternative payment methods (APMs) – GPE provider

The GP webpay system provides some other alternative payment methods.

The availability of methods is limited by their support on the part of the provider.

Available methods:

Payment institution	Value for field „PAYMETHOD“
All available merchant APM payment methods	APM-BTR

Czech Republic	
Platební instituce	**Value for field „PAYMETHOD“**
Česká spořitelna	APM-BCCS
Komerční banka	APM-BCKB
ČSOB CZ	APM-BCOB
Raiffesenbank	APM-BCRB
mBank	APM-BCMB
Fio banka	APM-BCFI
Moneta Bank	APM-BCMO
Air Bank	APM-BCAI
QR platba (its availability has to be verified)	APM-BCQR

Austria	
Payment institution	**Value for field „PAYMETHOD“**
EPS	APM-BAEB

Slovak Republic

Payment institution	Value for field „PAYMETHOD“
Slovenská sporiteľňa	APM-BSSS
Tatra Banka	APM-BSTB
VÚB banka	APM-BSVB
ČSOB SK	APM-BSOB
Prima banka	APM-BSPR
QR platba (Pay By Square) (its availability has to be verified)	APM-BSQR

The "PAYMETHOD" field can be used to directly select the desired method:

Parameter	Type	Length	Mandatory	Note
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. Supported values (see tables above) - Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields

8.4 Click To Pay (Click2Pay)

A payment method supported by card schemes (Mastercard, Visa) that allows a payment card to be stored/tokenized in a secure wallet according to the EMV Secure Remote Commerce standard.

The availability of methods is limited by their support on the part of the provider.

Parameter	Type	Length	Mandatory	Note
PAYMETHOD **field included in digest**	character	255	no	Value indicating the preferred payment method. Supported values: Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields **CTP – Click To Pay**

9. Payments facilitating functionalities

9.1 Recurring payment

9.1.1 Registration payment

The first one, the so-called registration payment, is made as a standard payment 3D Secure and the card holder has to be verified in that and the payment has to be made. Then the recurring payment can be created.

Registration payment is marked by adding the “USERPARAM1” parameter to the request:

Parameter	Type	Length	Mandatory	Note
USERPARAM1 **field included in digest**	character	255	yes/no *mandatory for registration of the “master” payment, otherwise not*	User’s field. Now used for submission of “R” parameter – information about a request for registration of “master” recurring payment.

Parameter	Type	Length	Mandatory	Note
			compulsory	

This parameter is located/chained behind the MD parameter.
Response format is identical to a standard format.

9.1.2 Recurring payment

Recurring payment is made using the API WS (Web Services) without redirecting of the customer's browser to the payment page for entering payment card data (see the technical specification for developers "GP webpay API WS").

9.2 Stored card (card on file [COF] payments – tokens)

9.2.1 Registration payment – payment card data tokenization

The first one, the so-called registration/tokenization payment, is made as a standard payment 3D Secure and the card holder has to be verified in that and the payment has to be made. Then the token payment can be created.

Tokens (card on file) should always be registered using the "`CARD_VERIFICATION`" operation (see chapter "Card verification").

Registration using payment with a minimum amount (1, - CZK / 0.10 EUR) and its subsequent reverse is no longer supported by card associations and will be penalized.

Registration with the first real payment (without reverse) is still allowed.

Registration/tokenization payment is marked by adding the "USERPARAM1" parameter to the request:

Parameter	Type	Length	Mandatory	Note
USERPARAM1 **field included in digest**	character	255	yes/no *mandatory for registration of the "master token" payment, otherwise not compulsory*	User's field. Now used for submission of "T" parameter – information about a request for token registration.

This parameter is located/chained behind the MD parameter.
Response format is identical to a standard format + payment card token and registration status is returned.

Value	Description
SUCCESS	Token has been successfully registered
EXISTOWNER	The card has already been registered and the token has been registered by the merchant requesting the registration
EXISTOTHER	The card has already been registered and the token has been registered by another merchant in the group

9.2.2 Token payment

Token payment is made using the API WS (Web Services) without redirecting of the customer's browser to the payment page for entering payment card data (see the technical specification for developers "GP webpay API WS").

9.3 Fasttoken

Fasttoken feature enables the merchant to display on the payment page for the logged in customer last 4 digits of the payment card and the card validity of the card, which the customer has used for the registration payment.

To integrate e-shop for this case of use, the "FASTTOKEN" parameter with value "TOKEN" from the registration payment request:

Parameter	Type	Length	Mandatory	Note
FASTTOKEN **field included in digest**	character	64	yes/no *mandatory if the Fasttoken service is used*	Unique identifier of the payment card calculated by the GP webpay system

If the relevant payment is not found, data are not displayed.

This parameter is located/chained behind the MD parameter.

Response format is identical to a standard format.

9.4 Fastpay

Fastpay feature enables the merchant to display on the payment page for the logged in customer last 4 digits of the payment card and the card validity of the card, which the customer has used for the previous payment.

To integrate e-shop for this case of use, the "FASTPAYID" parameter with value "ORDERNUMBER" from the previous payment is used in the request:

Parameter	Type	Length	Mandatory	Note
FASTPAYID **field included in digest**	numeric	15	yes/no *mandatory if the Fastpay service is used*	A unique ORDERNUMBER of the order, which was used in the past and should serve as a basis to pre-fill card number. The order should be paid and cannot be older than 12 (18) months, as it may have been automatically removed from the system.

If the relevant payment is not found, data are not displayed.

This parameter is located/chained behind the MD parameter.

Response format is identical to a standard format.

9.5 Stored card 3D

When the parameters "FASTPAYID" or "FASTTOKEN" and "USERPARAM1" are used, the GP webpay system can skip payment page and continue directly to 3D verification without request for CVC2/CVV2 data.

Parameter	Type	Length	Mandatory	Note
USERPARAM1 **field included in digest**	character	255	yes/no *mandatory for registration of the "master token" payment, otherwise not compulsory*	User's field. Now used for submission of "S" parameter – request for payment page skipping.

If the previous payment is not found the cardholder is returned to e-shop and the standard return code is provided. In case of expired card the return code is PRCODE=32.

Response format is identical to a standard format.

9.6 Card number pattern/token verification functionality

The GP webpay system allows to verify the typed-in payment card number against the pattern received in the request (PANPATTERN parameter) or against the token received in the request (TOKEN parameter). The token value is calculated after the first use of the payment card and is returned in the return parameter of the response. In combination with the VRCODE parameter it is possible to verify the linkage between the cardholder and the bank account.

The set of output parameters is extended at the same time.

9.6.1 Input parameters

Parameter	Type	Length	Mandatory	Note
VRCODE **field included in digest**	character	48	yes/no *mandatory field in case of the sending verification code in merchant's name to the AC*	Field for verification code, which is sent to the authorization center and displayed within the customer's internet banking. Character field in length max. 22 **BEFORE** encrypting. Encryption is made by means of the AES algorithm in CBC mode with "0000000000000000" (16x byte 0) initialization vector and PKCS5 padding. The result is converted by means of bin data into hex system; the output is in the form of text – i.e. each byte is represented by two characters in the range 00-FF.

This parameter is located/chained behind the MD parameter.

Parameter	Type	Length	Mandatory	Note
PANPATTERN **field included in digest**	character	255	no	To verify the typed-in payment card number (PAN) in the form at the payment gateway, it is possible to send up to 10 different "masks" of payment cards. Values are separated by commas ",". The verification is carried out when the PAN is typed-in at the gateway, or when Fastpay function is used. The mask can contain following values: {6}*{4} – first 6 digits of PAN, followed by **one character** "*", last 4 digits of PAN. PAN length is not checked. {6}******{4} – first 6 digits of PAN, followed by

Parameter	Type	Length	Mandatory	Note
				more characters "*", last 4 digits of PAN. PAN length is checked. {6}* – first 6 digits of PAN, followed by **one character** "*".PAN length is not checked. *{4} – **one character** "*",last 4 digits of PAN. PAN length is not checked.
TOKEN **field included in digest**	character	64	no	Unique identifier of the payment card calculated by the GP webpay system.

These parameters are located/chained behind the ADDINFO parameter.

9.6.2 Output parameters

Parameter	Type	Length	Mandatory	Note
TOKEN **field included in digest**	character	64	no	Unique identifier of the payment card calculated by the GP webpay system
EXPIRY **field included in digest**	character	4	no	Expiry date of the used payment card in the YYMM format
ACSRES **field included in digest**	character	1	no	Authentication result of the cardholder in the 3D system Possible values: N = an attempt for authentication has not been made – some card associations do not support 3D authentication A = an attempt for authentication has been made, however the card does not participate in the 3D system or the bank does not support the system F = the cardholder is fully authenticated D = the card has not been authenticated successfully (declined) – wrong authentication data E = technical problem with cardholder's authentication
ACCODE **field included in digest**	character	6	no	Authorization code of the payment obtained from the authorization center
PANPATTERN **field included in digest**	character	20	no	Masked number of the payment card used in the 6{***}4 format
DAYTOCAPTURE **field included in digest**	character	8	no	Date, until when capture can be made (for payments created with DEPOSITFLAG=0) Format: DDMMYYYY

These parameters are located/chained behind the ADDINFO parameter.

10. Annexes and addenda

10.1 Annex no. 1 – Signing messages

Annex moved to document

„**GP_webpay_Private_key_management_and_Signing_messages_vx.x_CZ/EN.docx**“.

10.2 Annex no. 2 – List of return codes

The result of the processing of the request in GP webpay is described as a pair of return codes. If these return codes are different from zero PRCODE describes the type of error. If SRCODE is different from zero it describes the error in detail.

The current list of all return codes can be found in the "Download" section of the GP webpay Portal - https://portal.gpwebpay.com in the document "GP webpay - List of return codes".

Example:

PRCODE=1 SRCODE=8 means that the DEPOSITFLAG field in the request received has been too long. The RESULTTEXT code returned in this case is “Field too long, DEPOSITFLAG”.

10.2.1 PRCODE / primaryReturnCode

PRCODE / primaryReturnCode		
Value	**Meaning CZ**	**Meaning EN**
0	OK	OK
1	Pole příliš dlouhé	Field too long
2	Pole příliš krátké	Field too short
3	Chybný obsah pole	Incorrect content of field
4	Pole je prázdné	Field is null
5	Chybí povinné pole	Missing required field
6	Pole neexistuje	Missing field
7	Chybná struktura WS požadavku SOAP zprávu nelze ověřit proti XSD šabloně. Detailní popis chyby je v odpovědi v elementu „<faultstring>“.	Wrong WS request structure SOAP request could not be verified against the XSD template. A detailed description is in the “<faultstring>” element.
	<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Body> <soapenv:Fault> <faultcode>soapenv:Server</faultcode> **<faultstring>Value 'SK' is not facet-valid with respect to pattern '\d{1,3}' for type 'CountryValue'.</faultstring>** <detail> <ns4:paymentServiceException xmlns:ns4="http://gpe.cz/pay/pay-ws/proc/v1" xmlns="http://gpe.cz/gpwebpay/additionalInfo/response" xmlns:ns2="http://gpe.cz/pay/pay-ws/core/type" xmlns:ns3="http://gpe.cz/pay/pay-ws/proc/v1/type" xmlns:ns5="http://gpe.cz/gpwebpay/additionalInfo/response/v1"> <ns3:messageId>Akj17dh61b11b6bd5d0d</ns3:messageId>	

```
            <ns3:primaryReturnCode>7</ns3:primaryReturnCode>
            <ns3:secondaryReturnCode>0</ns3:secondaryReturnCode>
                                        <ns3:signature>uhhvkmQAh …</ns3:signature>
                                    </ns4:paymentServiceException>
                                </detail>
                            </soapenv:Fault>
                        </soapenv:Body>
</soapenv:Envelope>
```


11	Neznámý obchodník	Unknown merchant
14	Duplikátní číslo platby	Duplicate order number
15	Objekt nenalezen	Object not found
16	Částka k autorizaci překročila původní částku platby	Amount to approve exceeds payment amount
17	Částka k zaplacení překročila povolenou (autorizovanou) částku	Amount to deposit exceeds approved amount
18	Součet vracených částek překročil zaplacenou částku	Total sum of credited amounts exceeded deposited amount
20	Objekt není ve stavu odpovídajícím této operaci *Info: Pokud v případě vytváření platby (CREATE_ORDER) obdrží obchodník tento návratový kód, vytvoření platby již proběhlo a platby je v určitém stavu – tento návratový kód je zapříčiněn aktivitou držitele karty (například pokusem o přechod zpět, použití refresh…).*	Object not in valid state for operation
25	Uživatel není oprávněn k provedení operace	Operation not allowed for user
26	Technický problém při spojení s autorizačním centrem	Technical problem in connection to authorization center
27	Chybný typ platby	Incorrect payment type
28	*Zamítnuto v 3D* *Info: důvod zamítnutí udává SRCODE*	Declined in 3D
30	*Zamítnuto v autorizačním centru* *Info: Důvod zamítnutí udává SRCODE*	Declined in AC
31	Chybný podpis	Wrong digest
32	Expirovaná karta	Expired card
33	Originální/Master platba není autorizovaná	Original/Master order was not authorized
34	Originální/Master platbu nelze použít pro následné platby	Original/Master order is not valid for subsequent payment
35	Expirovaná session Nastává při vypršení webové session při zadávání karty	Session expired
37	Karta na blacklistu – vydavatel zakázal další použití této karty	Blacklisted card - the issuer has banned further use of this card
38	Nepodporovaná karta	Card not supported
39	Karta na watchlistu – je povoleno max. 15 pokusů během posledních 30 dní	Watchlisted card - max 15 attempts allowed in the last 30 days
40	Zamítnuto ve Fraud detection system	Declined in Fraud detection system
46	Zamítnuto v Transaction analysis system (TRA)	Declined in Transaction analysis system (TRA)

50	Držitel karty zrušil platbu	The cardholder canceled the payment
80	Duplicitní MessageId	Duplicate MessageId
82	V HSM chybí název šifrovacího klíče	HSM key label missing
83	Operace zrušena vydavatelem	Canceled by issuer
84	Duplicitní hodnota	Duplikate value
85	Zakázáno na základě pravidel obchodníka	Declined due to merchant's rules
86	Podmíněně zamítnuto – vydavatel požaduje SCA	Soft decline – issuer requires SCA
150	PUSH platba nenalezena	PUSH payment not found
151	PUSH platba je po době platnosti	PUSH payment expired
152	PUSH platba již byla uhrazena	PUSH payment already paid
153	PUSH platba byla zrušena	PUSH payment revoked
154	PUSH platba není v odpovídající stavu této operaci	PUSH payment not in valid state for operation
155	PUSH platby nejsou povoleny	PUSH payment is not allowed by configuration
156	PUSH platba – překročen počet pokusů o úhradu	PUSH payment – number of payments exceeded
160	PUSH platba – požadovaná doba platnosti je chybná	PUSH payment – invalid requested expiration
161	Nelze znova použít PUSH link, protože stejná PUSH platba právě probíhá. Je potřeba dokončit původní platbu, nebo vyčkat na expiraci právě probíhající webové session (cca. 15 minut)	You cannot use the PUSH link again because the same PUSH payment is in progress. It is necessary to complete the original payment or wait for the expiration of the ongoing web session (approx. 15 minutes)
200	Žádost o doplňující informace	Additional info request
250	Požadavek nelze zpracovat, protože platba stále probíhá	Request cannot be processed as payment is still pending
500	Došlo ke ztrátě právě probíhající webové session	A web session in progress has been lost
501	Právě probíhající ztracená webová session byla obnovena	The lost web session in progress has been restored
502	Neočekávaný požadavek	Unexpected request
503	Nebylo zasláno webové session ID. Nelze dále pokračovat ve zpracování požadavku.	No web session ID has been sent. Cannot continue processing the request.
1000	Technický problém	Technical problem

10.2.2 SRCODE / secondaryReturnCode

SRCODE / secondaryReturnCode		
Value	**Meaning CZ**	**Meaning EN**
0	Bez významu	No meaning
If PRCODE is 1 to 5, 15 and 20, the following SRCODE may return		
1	ORDERNUMBER	ORDERNUMBER
2	MERCHANTNUMBER	MERCHANTNUMBER
3	PAN	PAN
4	EXPIRY	EXPIRY

5	CVV	CVV
6	AMOUNT	AMOUNT
7	CURRENCY	CURRENCY
8	DEPOSITFLAG	DEPOSITFLAG
10	MERORDERNUM	MERORDERNUM
11	CREDITNUMBER	CREDITNUMBER
12	OPERATION	OPERATION
14	ECI	ECI
18	BATCH	BATCH
22	ORDER	ORDER
24	URL	URL
25	MD	MD
26	DESC	DESC
34	DIGEST	DIGEST
38	LANG	LANG
43	ORIGINAL ORDER NUMBER	ORIGINAL ORDER NUMBER
45	USERPARAM1	USERPARAM1
70	VRCODE	VRCODE
71	USERPARAM2	USERPARAM2
72	FASTPAYID	FASTPAYID
73	PAYMETHOD	PAYMETHOD
76	PAYMETHOD_DISABLED	PAYMETHOD_DISABLED
77	EMAIL	EMAIL
83	ADDINFO	ADDINFO
84	MPS_CHECKOUT_ID	MPS_CHECKOUT_ID
85	SHIPPING_LOCATION_RESTRICTION	SHIPPING_LOCATION_RESTRICTION
86	PAYMETHODS	PAYMETHODS
87	REFERENCENUMBER	REFERENCENUMBER
88	DEPOSIT_NUMBER	DEPOSIT_NUMBER
89	RECURRING_ORDER	RECURRING_ORDER
90	PAIRING / TRACE_ID	PAIRING / TRACE_ID
91	SHOP_ID	SHOP_ID
92	PANPATTERN	PANPATTERN
93	TOKEN	TOKEN
95	FASTTOKEN	FASTTOKEN
96	SUBMERCHANT INFO	SUBMERCHANT INFO
97	TOKEN_HSM_LABEL	TOKEN_HSM_LABEL

98	CUSTOM INSTALLMENT COUNT	CUSTOM INSTALLMENT COUNT
99	COUNTRY	COUNTRY
100	TERMINAL INFO	TERMINAL INFO
101	TERMINAL ID	TERMINAL ID
102	TERMINAL OWNER	TERMINAL OWNER
103	TERMINAL CITY	TERMINAL CITY
104	MC ASSIGNED ID	MC ASSIGNED ID
300	Podmíněně zamítnuto – vydavatel požaduje SCA	Soft decline – issuer requires SCA
If PRCODE is 28, the following SRCODE may return		
3000	Neověřeno v 3D. Vydavatel karty není zapojen do 3D nebo karta nebyla aktivována. *Info: Ověření držitele karty bylo neúspěšné (neplatně zadané údaje, stornování autentikace, uzavření okna pro autentikaci držitele karty se zpětnou vazbou…).* *V transakci se nesmí pokračovat.*	Declined in 3D. Cardholder not authenticated in 3D. *Note: Cardholder authentication failed (wrong password, transaction canceled, authentication window was closed…).* *Transaction Declined.*
3001	Držitel karty ověřen. *Info: Ověření držitele karty v 3D systémech proběhlo úspěšně. Pokračuje se autorizací platby.*	Authenticated *Note: Cardholder was successfully authenticated – transaction continue with authorization.*
3002	Neověřeno v 3D. Vydavatel karty nebo karta není zapojena do 3D. *Info: V 3D systémech nebylo možné ověřit držitele karty – karta, nebo její vydavatel, není zapojen do 3D.* *V transakci se pokračuje.*	Not Authenticated in 3D. Issuer or Cardholder not participating in 3D. *Note: Cardholder wasn't authenticated – Issuer or Cardholder not participating in 3D.* *Transaction can continue.*
3004	Neověřeno v 3D. Vydavatel karty není zapojen do 3D nebo karta nebyla aktivována. *Info: V 3D systémech nebylo možné ověřit držitele karty – karta není aktivována, nebo její vydavatel, není zapojen do 3D.* *V transakci je možné pokračovat.*	Not Authenticated in 3D. Issuer not participating or Cardholder not enrolled. *Note: Cardholder wasn't authenticated – Cardholder not enrolled or Issuer or not participating in 3D.* *Transaction can continue.*
3005	Zamítnuto v 3D.Technický problém při ověření držitele karty. *Info: V 3D systémech nebylo možné ověřit držitele karty – vydavatel karty nepodporuje 3D, nebo technický problém v komunikaci s 3D systémy finančních asociací, či vydavatele karty.* *V transakci není možné pokračovat, povoleno z důvodu zabezpečení obchodníka před případnou reklamací transakce držitelem karty.*	Declined in 3D. Technical problem during Cardholder authentication. *Note: Cardholder authentication unavailable – issuer not supporting 3D or technical problem in communication between associations and Issuer 3D systems.* *Transaction cannot continue.*
3006	Zamítnuto v 3D. Technický problém při ověření držitele karty.	Declined in 3D. Technical problem during Cardholder authentication.

	Info: V 3D systémech nebylo možné ověřit držitele karty – technický problém ověření obchodníka v 3D systémech, anebo v komunikaci s 3D systémy finančních asociací, či vydavatele karty. *V transakci není možné pokračovat.*	*Note: Technical problem during cardholder authentication – merchant authentication failed or technical problem in communication between association and acquirer.* *Transaction cannot continue.*
3007	Zamítnuto v 3D. Technický problém v systému zúčtující banky. Kontaktujte obchodníka. *Info: V 3D systémech nebylo možné ověřit držitele karty – technický problém v 3D systémech.* *V transakci není možné pokračovat.*	Declined in 3D. Acquirer technical problem. Contact the merchant. *Note: Technical problem during cardholder authentication – 3D systems technical problem.* *Transaction cannot continue.*
3008	Zamítnuto v 3D. Použit nepodporovaný karetní produkt. *Info: Byla použita karta, která není v 3D systémech podporována.* *V transakci není možné pokračovat.*	Declined in 3D. Unsupported card product. *Note: Card not supported in 3D.* *Transaction cannot continue.*
If PRCODE is 30, the following SRCODE may return		
1001	**Zamitnuto v autorizacnim centru, karta blokovana**[1] *Zahrnuje důvody, které naznačují zneužití platební karty – kradená karta, podezření na podvod, ztracená karta apod.* *Karta je označena jako:* *Ztracená* *K zadržení* *K zadržení (speciální důvody)* *Ukradená* *Většinou pokus o podvodnou transakci.*	Declined in AC, Card blocked *It includes reasons that indicate misuse of t It includes reasons that indicate misuse of the payment card - stolen card, suspected fraud, lost card, etc.* *The card is marked as:* *Lost* *To be detained* *To be detained (special reasons)* *Stolen* *Usually an attempted fraudulent transaction.*
1002	**Zamitnuto v autorizacnim centru, autorizace zamítnuta** *Z autorizace se vrátil důvod zamítnutí "Do not honor".* *Vydavatel, nebo finanční asociace zamítla autorizaci BEZ udání důvodu.*	Declined in AC, Declined *The "Do not honor" rejection reason was returned from the authorization.* *The publisher or financial association rejected the authorization WITHOUT giving a reason.*
1003	**Zamitnuto v autorizacnim centru, problem karty** *Zahrnuje důvody:* *expirovaná karta, chybné číslo karty, nastavení karty - pro kartu není povoleno použití na internetu, nepovolená karta, expirovaná karta, neplatná karta, neplatné číslo karty, částka přesahuje maximální limit karty, neplatné CVC/CVV, neplatná délka čísla karty, neplatná expirační doba, pro kartu je požadována kontrola PIN.*	Declined in AC, Card problem *Includes reasons:* *Expired card, incorrect card number, card settings - no internet use allowed for card, unauthorized card, expired card, invalid card, invalid card number, amount exceeds maximum card limit, invalid CVC/CVV, invalid card number length, invalid expiration date, PIN check required for card.*
1004	**Zamitnuto v autorizacnim centru, technicky problem** *Autorizaci není možné provést z technických*	Declined in AC, Technical problem in authorization process *Authorization cannot be performed for technical*

[1]Only the bold part in this and the following cells of this column will be included in the RESULTTEXT field (optional field) in a response sent to the merchant. Other text is only the explanation for merchants.

	důvodů – technické problémy v systému vydavatele karty, nebo finančních asociací a finančních procesorů.	*reasons - technical problems in the card issuer's system or financial associations and financial processors.*
1005	**Zamitnuto v autorizacnim centru, Problem uctu** *Důvody: nedostatek prostředků na účtu, překročeny limity, překročen max. povolený počet použití…*	Declined in AC, Account problem *Reasons: insufficient funds in the account, limits exceeded, maximum number of uses...*
1012	**Zamitnuto v autorizacnim centru, Karta na blacklistu** *Vydavatel zakázal další použití této karty*	Declined in AC, Blacklisted card *The issuer has banned further use of this card*
1013	**Zamitnuto v autorizacnim centru, Karta na watchlistu** *Je povoleno max. 15 pokusů během posledních 30 dní*	Declined in AC, Watchlisted card *Max 15 attempts allowed in the last 30 days*

If authorization is rejected, the payment gateway receives the return code directly from the card issuer (or from the service provider, or financial association). If the rejected authorization is claimed, the cardholder has to contact his card issuing bank, which responses him directly, or this bank resolves a claim with the bank, which processed the transaction (merchant's bank).

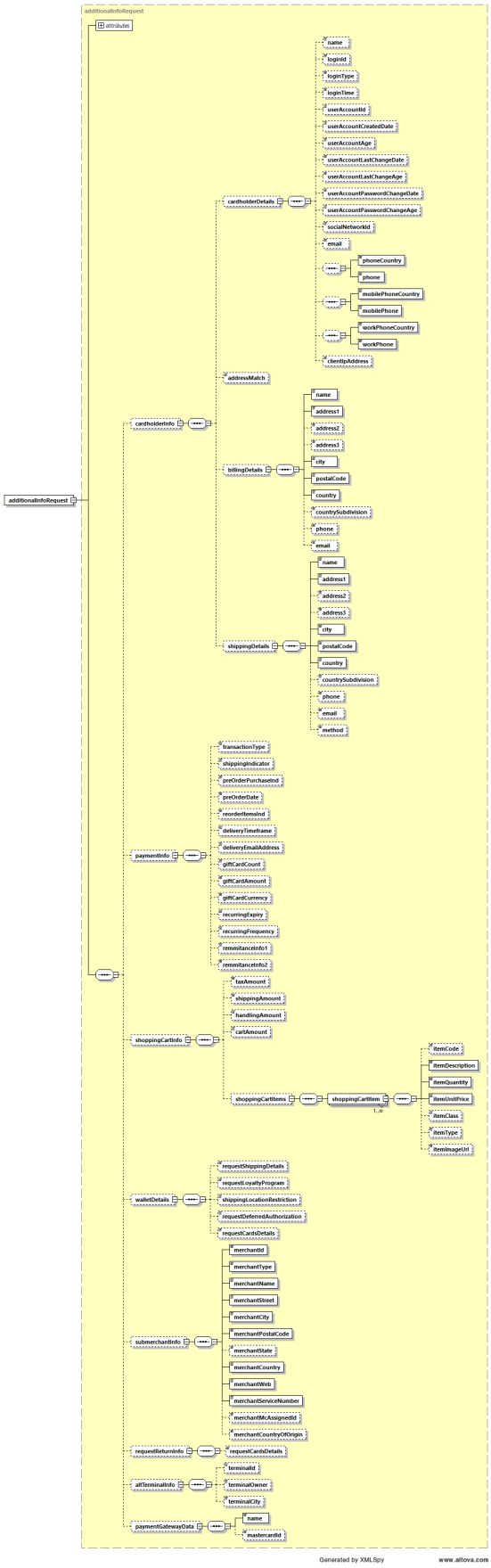
10.3 Annex no. 3 – ADDINFO field format

List of element types

Type name	Description
Composite type	The element is composed of more elements of various types.
Co-linked type	The object consists of multiple elements. It is always necessary to disable either all elements marked as bound or none. **It is not possible to fill only some of them, even if they are marked as optional.**
Amount	The number of max. 12 digits. The value must be stated in the smallest monetary unit of a given currency without decimal point.

10.3.1 Input parameter “ADDINFO” – version 5

10.3.1.1 Elements description



Element	Description	M/O[2]	Type
additionalInfoRequest	The main element containing all requested information.	M	A composite type
version="x.x"	*A component part is an attribute containing information about version of the used template.* **Depending on the version, the appropriate template is selected on the server and validation is performed.**	*M*	*Numeric type in the format e.g. "1.0".* **Current version is "5.0"**
Customer´s data used in the anti-fraud system			
cardholderInfo	Cardholder information	O	A composite type
cardholderDetails	Basic information about cardholder	O	A composite type
name	Card holder name	O	Text, max. 45 characters ASCII x20-x7E
loginId	LoginID into e-shopu	O	Text, max. 255 characters
loginType	Mechanism used by the Cardholder to authenticate to the e-shop.	O	Values accepted: • 01 = No merchant authentication occurred (i.e. cardholder "logged in" as guest) • 02 = Login to the cardholder account at the merchant system using merchant's own credentials • 03 = Login to the cardholder account at the merchant system using federated ID • 04 = Login to the cardholder account at the merchant system using issuer credentials • 05 = Login to the cardholder account at the merchant system using third-party authentication • 06 = Login to the cardholder account at the merchant system using FIDO Authenticator • 07–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80–99 = Reserved for DS use
loginTime	Date and time in UTC of the cardholder authentication.	O	Date, format: YYYYMMDDHHMM
userAccountId	User account ID in the e-shop system	O	Text, max. 64 characters
userAccountCreatedDate	Date that the cardholder opened the account with the merchant.	O	Date, format: YYYYMMDD
userAccountAge	Length of time that the cardholder has had the account with the merchant.	O	• 01 = No account (guest check-out) • 02 = Created during this transaction • 03 = Less than 30 days • 04 = 30−60 days • 05 = More than 60 days

[2] M – mandatory, O – optional

userAccountLastChangeDate	Date that the cardholder's account with the merchant was last changed, including Billing or Shipping address, new payment account, or new user(s) added.	O	Date, format: YYYYMMDD
userAccountLastChangeAge	Length of time since the cardholder's account information with the merchant was last changed, including Billing or Shipping address, new payment account, or new user(s) added.	O	• 01 = Changed during this transaction • 02 = Less than 30 days • 03 = 30−60 days • 04 = More than 60 days
userAccountPasswordChangeDate	Date that cardholder's account with the merchant had a password change or account reset.	O	Date, format: YYYYMMDD
userAccountPasswordChangeAge	Indicates the length of time since the cardholder's account with the merchant had a password change or account reset.	O	• 01 = No change • 02 = Changed during this transaction • 03 = Less than 30 days • 04 = 30−60 days • 05 = More than 60 days
socialNetworkId	LoginID into e-shop if used login via social network (Facebook, Google ...)	O	Text, max. 255 characters
email	Card holder's e-mail	O	E-mail, max. 255 characters
Co-linked type			
phoneCountry	Phone number country code	O[3]	Number, 3 characters Format: country code (420)
phone	Phone number	O[3]	Number, 15 characters Format: phone number (123456789)
Co-linked type			
mobilePhoneCountry	Phone number country code	O[3]	Number, 3 characters Format: country code (420)
mobilePhone	Mobile phone number	O[3]	Text, 15 characters Format: phone number (123456789)
Co-linked type			
workPhoneCountry	Phone number country code	O[3]	Number, 3 characters Format: country code (420)

[3] If phone number is filled in, the phone country code must be provided, too.

workPhone	Mobile phone number	O[3]	Text, 15 characters Format: phone number (123456789)
clientIpAddress	Card holder's IP address	O	Text, max. 255 characters
addressMatch	Indicates whether the Cardholder Shipping Address and Cardholder Billing Address are the same.	O	• Y = Shipping Address matches Billing Address • N = Shipping Address does not match Billing Address
billingDetails	Billing address	O	A composite type
name	Name	M	Text, max. 255 characters
address1	Street – 1. line	M	Text, max. 50 characters
address2	Street – 2. line	O	Text, max. 50 characters
address3	Street – 3. line	O	Text, max. 50 characters
city	City	M	Text, max. 50 characters
postalCode	Postal code / ZIP	M	Text, max. 16 characters
country	Country	M	Number, max. 3 characters Country list: ISO 3166-1
countrySubdivision	Country subdivision	O	Number, max. 3 characters Country list: ISO 3166-2
phone	Phone number	O	Text, max. 20 characters
email	E-mail	O	E-mail, 6-255 characters
shippingDetails	Shipping address	O	A composite type
name	Name	M	Text, max. 255 characters
address1	Street – 1. line	M	Text, max. 50 characters
address2	Street – 2. line	O	Text, max. 50 characters
address3	Street – 3. line	O	Text, max. 50 characters
city	City	M	Text, max. 50 characters
postalCode	Postal code / ZIP	M	Text, max. 16 characters
country	Country	M	Number, max. 3 characters Country list: ISO 3166-1
countrySubdivision	Country subdivision	O	Number, max. 3 characters Country list: ISO 3166-2

phone	Phone number	O	Text, max. 20 characters
email	E-mail	O	E-mail, 6-255 characters
method	Delivery method `personal pick-up, courier, electronic delivery …`	O	Text, max. 255 characters
Payment additional info			
paymentInfo	Additional payment info	O	A composite type
transactionType	Identifies the type of transaction being authenticated.	O	• 01 = Goods/ Service Purchase • 03 = Check Acceptance • 10 = Account Funding • 11 = Quasi-Cash Transaction • 28 = Prepaid Activation and Load
shippingIndicator	Indicates shipping method chosen for the transaction. Merchants must choose the Shipping Indicator code that most accurately describes the cardholder's specific transaction, not their general business. If one or more items are included in the sale, use the Shipping Indicator code for the physical goods, or if all digital goods, use the Shipping Indicator code that describes the most expensive item.	O	• 01 = Ship to cardholder's billing address • 02 = Ship to another verified address on file with merchant • 03 = Ship to address that is different than the cardholder's billing address • 04 = "Ship to Store" / Pick-up at local store (Store address shall be populated in shipping address fields) • 05 = Digital goods (includes online services, electronic gift cards and redemption codes) • 06 = Travel and Event tickets, not shipped • 07 = Other (for example, Gaming, digital services not shipped, emedia subscriptions, etc.)
preOrderPurchaseInd	Indicates whether Cardholder is placing an order for merchandise with a future availability or release date.	O	• 01 = Merchandise available • 02 = Future availability
preOrderDate	For a pre-ordered purchase, the expected date that the merchandise will be available.	O	Date, format: YYYYMMDDHHMM
reorderItemsInd	Indicates whether the cardholder is reordering previously purchased merchandise.	O	• 01 = First time ordered • 02 = Reordered
deliveryTimeframe	Indicates the merchandise delivery timeframe.	O	• 01 = Electronic Delivery • 02 = Same day shipping • 03 = Overnight shipping • 04 = Two-day or more shipping
deliveryEmailAddress	For Electronic delivery, the email address to which the merchandise was delivered.	O	E-mail, 6-255 characters
giftCardCount	For prepaid or gift card purchase, total count of individual prepaid or gift cards/codes	O	Number, 1-99

	purchased.		
giftCardAmount	For prepaid or gift card purchase, the purchase amount total of prepaid or gift card(s) in major units (for example, USD 123.45 is 123).	O	Number, 15 characters
giftCardCurrency	Currency code	O	Number, 3 characters ISO 4217 currency codes
recurringExpiry	Date after which no further authorizations shall be performed.	O	Date, format: YYYYMMDDHHMM
recurringFrequency	Indicates the minimum number of days between authorizations.	O	Number, 4 characters
remmitanceInfo1	Merchant can provide information about good (e.g. for airtickets - destination)	O	Text, max 140 characters
remmitanceInfo1	Merchant can provide information about good (e.g. for airtickets - destination)	O	Text, max 140 characters
Basket data used in the anti-fraud system and electronic wallets			
shoppingCartInfo	Element containing information about the basket	O	A composite type
taxAmount	VAT amount	O	Amount
shippingAmount	Shipping amount	O	Amount
handlingAmount	Handling amount	O	Amount
cartAmount	VAT-exlusive basket net value. Value is calculated as: `(shoppingCartItem1[itemQuantity] * shoppingCartItem1[itemUnitPrice]) + (shoppingCartItem2[itemQuantity] * shoppingCartItem2[itemUnitPrice]) + …`	O	Amount
shoppingCartItems	Individual items in the basket. It is possible to give more items.	M	A composite type
shoppingCartItem	Basket item	M	A composite type
itemCode	Item code, e.g. "item 1"	O	Text, max. 20 characters
itemDescription	Item description	M	Text, max. 50 characters
itemQuantity	Number of items	M	Number, max. 12 numbers
itemUnitPrice	VAT-exclusive unit price	M	Amount

itemClass	Item class, e.g. "class A"	O	Text, max. 20 characters
itemType	Item type, e.g. "men´s clothing"	O	Text, max. 20 characters
itemImageUrl	Complete URL path to item picture. When using wallet, an item picture could be shown next to the item.	O	URL, max. 2000 characters
Data section when using any of electronic wallets			
walletDetails	Element adjusting possibilities of the wallet	O	A composite type
requestShippingDetails	Switch defining, if information about delivery address is demanded in the response	O	true/false
requestLoyaltyProgram	Switch defining, if information about loyalty programme is demanded in the response	O	true/false
shippingLocationRestriction	List of countries supported for delivery	O	Limitation of delivery address choice. Supported values: CZ – Czech Republic SK – Slovakia HU – Hungary EU – European Union US – USA WW – whole world (no limits) Default value is set according to the bank seat. In case of a request to deliver to other countries, please contact our application support.
requestDeferredAuthorization	Element setting to "true" enables to suspend payment processing in the GP webpay system and to request finalization data from the merchant	O	true/false
requestCardsDetails	Request for sending payment card/cards detail in the response	O	true/false
Data section for large payment services providers			
submerchantInfo	Information about merchant's realizing transactions through a payment aggregator (payment facilitator model)	O	A composite type
merchantId	A number assigned to each merchant	M	Max. 15 characters

			ASCII x20-x7E
merchantType	Merchant's MCC code	M	4 numbers
merchantName	Merchant name The final name of the merchant is a composite name aggregator and merchant	M	Max. 22 characters ASCII x20-x7E
merchantStreet	Street	M	Max. 25 characters ASCII x20-x7E
merchantCity	City	M	Max. 13 characters ASCII x20-x7E
merchantPostalCode	Postal code / ZIP	M	Max. 10 characters
merchantState	State	O	Max. 3 characters
merchantCountry	Country code – ISO 3166-1 Alpha-2	M	2 characters
merchantWeb	Merchant's web page URL	M	Max. 25 characters ASCII x20-x7E
merchantServiceNumber	Merchant's phone number – customer support	M	13 numbers
merchantMcAssignId	ID assigned by Mastercard for public institutions	O	Text, 15 characters
merchantCountryOfOrigin	Country code – ISO 3166-1 numeric MC mandates "Country of Origin" **for government owned merchants.**	O	For **government owned merchants**, this value must always be filled in, even if the country of the merchant is the same as the country of the owner. MC checks these MCCs (Edit 24/34): 9211 (Court costs including alimony and child support) 9222 (Fines) 9311 (Tax payments) 9399 (Government services - not elsewhere classified) 9402 (Postal services - government only) 9405 (Intra-government purchases-government only) 9406 (Government-owned lottery [Global, excluding US region]) E.g.: ***Czech Post*** – Czech Republic owned merchant – MCC 9402 (Postal services - government only): 203 - Czech Republic

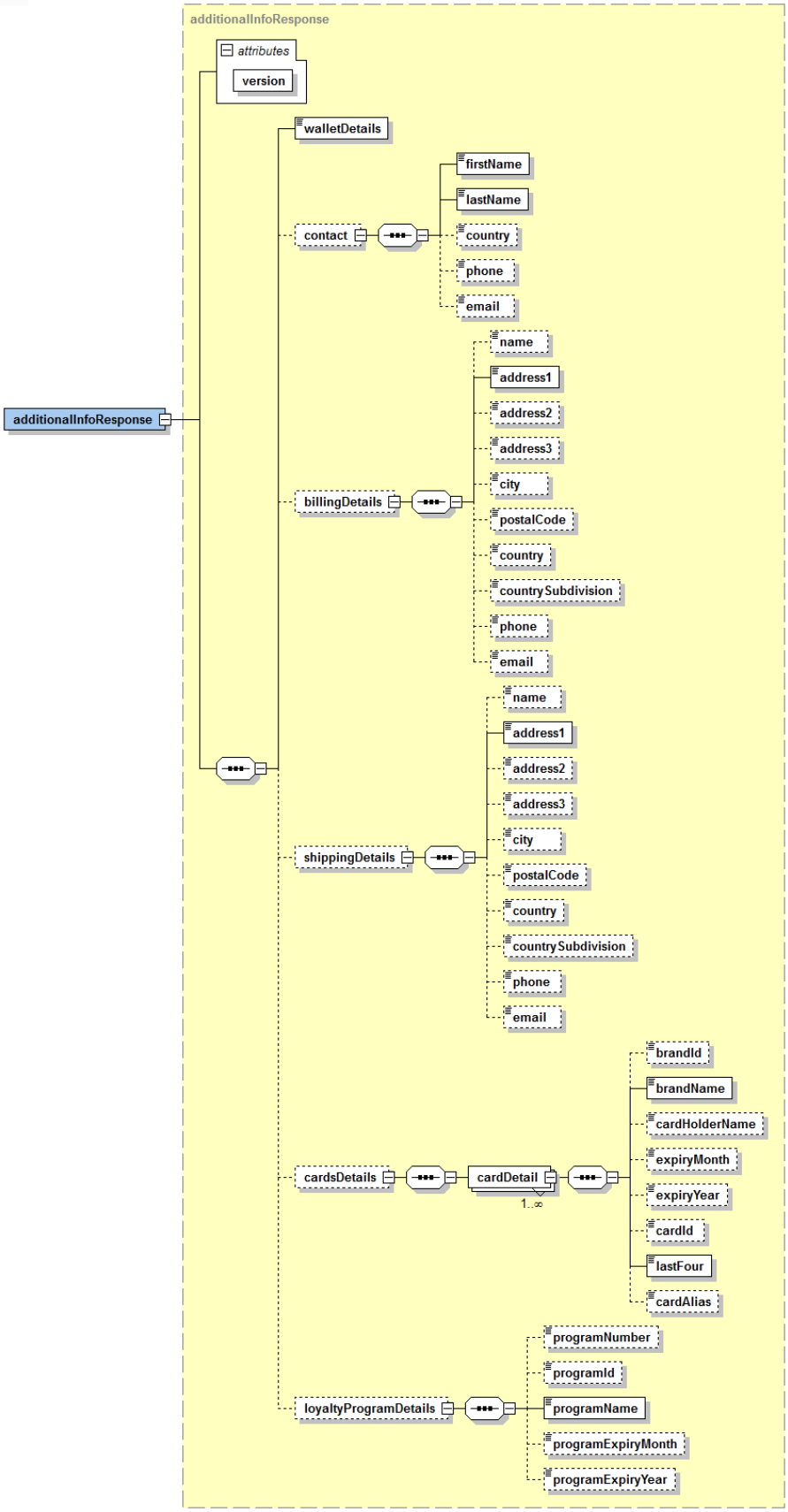
			Australian Embassy – Australia owned merchant - MCC 9399 (Government services - not elsewhere classified): 036 - Australia The flagging is not limited to the above MCCs, but applies to **all government owned merchants** – e.g.: ***Czech Railways*** – Czech Republic owned merchant – MCC 4789 (TRANSPORTATION SERVICES): 203 - Czech Republic Supported values: 3 numbers
Request for additional information in response			
requestReturnInfo	Request for additional information in response	O	A composite type
requestCardsDetails	Request for used card information	O	true/false
Additional terminal info to the authorization center			
altTerminalInfo	Additional terminal info	O	A composite type
terminalId	Alternate terminal ID	O	Text, max. 8 characters
terminalOwner	Alternate terminal owner name	O	Text, max. 22 characters
terminalCity	Alternate terminal city location	O	Text, max. 13 characters
Additional information about the payment gateway – ONLY for merchants/PSP with own payment page			
paymentGatewayData	Additional information about the payment gateway	O	A composite type
name	The name of the gateway	P	Text, max. 50 characters ASCII x20-x7E (not starting with “space” character)
mastercardId	Merchant Payment Gateway ID (MPG ID) issued by Mastercard	O	Max. 11 numbers

10.3.1.2 Parameter scheme

XSD scheme file “**`GPwebpayAdditionalInfoRequest_v.x.xsd`**” can be found in the "Download" section of the GP webpay Portal - https://portal.gpwebpay.com.

10.3.2 Return parameter “ADDINFO”

10.3.2.1 Elements description



Element	Description	M/O	Type
additionalInfoResponse	The main element containing all requested information.	M	Composite type
version="x.x"	*A component part is an attribute containing information about version of the used template.*	*M*	*Numeric type in the format e.g. "1.0".*
Information about the used electronic wallet			
walletDetails	Information about the used wallet. Currently supported values : MPS	M	Text, max. 255 characters
Data gained from the electronic wallet			
contact	Cardholder info	O	Composite type
firstName	Name	M	Text, max. 255 characters
lastName	Surname	M	Text, max. 255 characters
country	Country	M	Text, max. 255 characters
phone	Phone	O	Text, max. 20 characters
email	E-mail	O	Text, max. 255 characters
billingDetails	Billing address	O	Composite type
name	Name	O	Text, max. 255 characters
address1	Street – 1. Line	M	Text, max. 255 characters
address2	Street – 2. Line	O	Text, max. 255 characters
address3	Street – 3. Line	O	Text, max. 255 characters
city	City	M	Text, max. 255 characters
postalCode	Postal code / ZIP	O	Text, max. 255 characters
country	Country	M	Text, max. 255 characters
countrySubdivision	Country subdivision	O	Text, max. 255 characters
phone	Phone	O	Text, max. 20 characters
email	E-mail	O	Text, max. 255 characters
shippingDetails	Shipping address	O	Composite type
name	Name	O	Text, max. 255 characters
address1	Street – 1. line	M	Text, max. 255 characters
address2	Street – 2. line	O	Text, max. 255 characters
address3	Street – 3. line	O	Text, max. 255 characters
city	City	M	Text, max. 255 characters
postalCode	Postal code / ZIP	O	Text, max. 255 characters
country	Country	M	Text, max. 255 characters
countrySubdivision	Country subdivision	O	Text, max. 255 characters
phone	Phone	O	Text, max. 20 characters
email	E-mail	O	Text, max. 255 characters
Data gained from the electronic wallet			
cardsDetails	Details about cards registered in electronic wallet and meeting conditions given in the input request.	O	Composite type
cardDetail	Card detail; there can be more of them (when using electronic wallet)	M	Composite type
brandId	Card association ID	O	Text, max. 255 characters
brandName	Name of the card association	M	Text, max. 255 characters
cardHolderName	Cardholder name	O	Text, max. 255 characters
expiryMonth	Month of card expiration	O	1-2 digits

expiryYear	Year of card expiration	O	4 digits
cardId	Card ID in the electronic wallet	O	Text, max. 255 characters
lastFour	Last 4 digits of the card number	M	4 digits
cardAlias	Card alias in the electronic wallet	O	Text, max. 255 characters
Data gained from the electronic wallet			
loyaltyProgramDetails	Information about loyalty programme	O	Composite type
programNumber	Programme number	O	Text, max. 255 characters
programId	Programme ID	O	Text, max. 255 characters
programName	Programme name	M	Text, max. 255 characters
programExpiryMonth	Month of programme termination	O	Number, 1-12
programExpiryYear	Year of programme termination	O	Number, 2014-2099

10.3.2.2 Parameter scheme

XSD scheme file "**`GPwebpayAdditionalInfoResponse_v.x.xsd`**" can be found in the "Download" section of the GP webpay Portal - https://portal.gpwebpay.com.

10.4 Annex no. 4 – Mandatory PSD2 data from the point of view of card schemes

Card schemes require the mandatory transmission of the data below for each card payment with the main goal of supporting the purchasing process as much as possible without interruption by authentication steps on the part of the issuer bank by applying the TRA (Transaction Risk Analysis) exception:

- Cardholder Name
- Email address **AND/OR** Home/Mobile/Work Phone Number[4]

This does not in any way affect the requirement to send the widest possible set of data that can be used for 3D authentication/verification in the Fraud Detection System of the cardholder - see the entire sections of the fields "cardHolderData", "paymentInfo", "shoppingCartInfo".

The data is not technically enforced in the XSD template, but is required by the card schemas. If some data is not available, it is not possible to use "made up" data and it is not possible to send a field blank (check for minimum length) - the field will not be sent at all.

This information will be refined according to further requirements of the card schemes.

It is necessary to correctly fill the structure of the `<cardholderInfo>` element:

Element	Description	M/O[5]	Note
cardholderInfo	Cardholder information	M	If any data from the list below exists, the element is mandatory.
cardholderDetails	Basic information about cardholder	M	If any data from the list below exists, the element is mandatory.
name	Card holder name	M	
email	Card holder's e-mail	M/O[4]	
Co-linked type	The object consists of multiple elements. It is always necessary to disable either all elements marked as bound or none. **It is not possible to fill only some of them, even if they are marked as optional.**		
phoneCountry	Phone number country code	M/O[4,6]	
phone	Phone number	M/O[4,6]	
Co-linked type			
mobilePhoneCountry	Phone number country code	M/O[4,6]	
mobilePhone	Mobile phone number	M/O[4,6]	
Co-linked type			
workPhoneCountry	Phone number country code	M/O[4,6]	
workPhone	Mobile phone number	M/O[4,6]	

[4] It is necessary to fill in an e-mail or at least one phone number. If both data exist, it is advisable to send both

[5] M – mandatory, O – optional

[6] If phone number is filled in, the phone country code must be provided, too.

billingDetails	Billing address	O	If any data from the list below exists, the element is mandatory.
name	Name	O	
address1	Street – 1. line	O	
address2	Street – 2. line	O	
address3	Street – 3. line	O	
city	City	O	
postalCode	Postal code / ZIP	O	
country	Country	O	ISO 3166-1
countrySubdivision	Country subdivision	O	ISO 3166-2

10.5 Annex no. 5 – List of values for the "PAYMETHOD" and "PAYMETHODS" fields

Description	Value for field „PAYMETHOD“, „PAYMETHODS“
Payment card	CRD
GooglePay	GPAY
ApplePay	APAY
PAYPAL	PAYPAL
Click To Pay	CTP
All available merchant APM payment methods	APM-BTR
APM – Czech Republic	
Česká spořitelna	APM-BCCS
Komerční banka	APM-BCKB
ČSOB CZ	APM-BCOB
Raiffesenbank	APM-BCRB
mBank	APM-BCMB
Fio banka	APM-BCFI
Moneta Bank	APM-BCMO
Air Bank	APM-BCAI
QR platba (its availability has to be verified)	APM-BCQR
APM – Austria	
EPS	APM-BAEB
APM – Slovak Republic	
Slovenská sporiteľňa	APM-BSSS
Tatra Banka	APM-BSTB
VÚB banka	APM-BSVB
ČSOB SK	APM-BSOB
Prima banka	APM-BSPR
QR platba (Pay By Square) (its availability has to be verified)	APM-BSQR
Support for the following methods will be reduced / terminated	

Description	Value for field „PAYMETHOD“, „PAYMETHODS“
Platba24 (Česká spořitelna)	*BTNCS*
Sofort	*SOFORT*
EPS	*EPS*
PAYSAFECARD	*PAYSAFECARD*
SEPADIRECTDEBIT	*SEPADIRECTDEBIT*
KLARNA	*KLARNA*

10.6 Addendum no. 1 – BASE64 encoding / decoding

Base64 is an encoding algorithm used to encode any binary data to a text form which can be easily printed and transmitted.

The result of the Base64 encoding can be transmitted without any risk of the data being converted and destroyed this way.

Base64 encoding uses the defined alphabet consisting of 65 US-ASCII characters (64 characters and space). See the following table:

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	A	17	R	34	i	51	z
1	B	18	S	35	j	52	0
2	C	19	T	36	k	53	1
3	D	20	U	37	l	54	2
4	E	21	V	38	m	55	3
5	F	22	W	39	n	56	4
6	G	23	X	40	o	57	5
7	H	24	Y	41	p	58	6
8	I	25	Z	42	q	59	7
9	J	26	a	43	r	60	8
10	K	27	b	44	s	61	9
11	L	28	c	45	t	62	+
12	M	29	d	46	u	63	/
13	N	30	e	47	v		
14	O	31	f	48	w	(pad)	=
15	P	32	g	49	x		
16	Q	33	h	50	y		

The source data are converted into the binary system as a flow of input bits (1 character equals 8 bits). The input flow is divided into groups of 6 bits and the values are converted according to the codes from the encoding table.

Every 3 input characters (3 x 8 = 24) are encoded as 4 output characters (24 / 6 = 4). If there are less then 24 bits at the end of the input data after it is divided, zero bits are appended to the input data from the right side. Zero bits appended to the input data are indicated with “=”.

Decoding of base64 encoded data is a process exactly reverted to base64 encoding. A flow of bits is extracted from the encoded data using the encoding table. The flow is then divided into groups of 8 bits, and the groups are converted back to the original form of the input data.

See RFC 3548 for a detailed description of base64 encoding.

10.7 Addendum no. 2 – Documentation and information sources

- ISO 639-1:2002 Codes for the representation of names of languages

  Part 1: Alpha-2 code
- ISO 639-2:1998 Codes for the representation of names of languages

  Part 2: Alpha-3 code
- ISO 4217:2001 Codes for the representation of currencies and funds
- RFC 3066 – Tags for the Identification of Languages

10.8 Addendum no. 3 – Maximum length of MERORDERNUM field

Maximum length of **MERORDERNUM** for particular banks as displayed in reports devoted for merchants:

Bank	Max. number of digits in MERORDERNUM displayed in the bank's report
Komerční banka	16
Raiffeisen bank	10
UniCredit bank	12
Danube Pay	16