GP webpay
Payment Gateway

User's guide

Version: 1.9
Global Payments Europe, s.r.o.
Created **31.5.2016**
Last update **14.7.2021**

SERVICE. DRIVEN. COMMERCE

globalpaymentsinc.com

Author	GPE Product
Manager	GPE Product
Approved by	
Version	1.9
Confidentiality	Confidential

Document history:

Version	Data	Author	Comment
0.1	31.05.2016	GPE Product	Initial document version – synthesis and revision of the following documents: GP_webpay_Popis_sluzby_v2.0 GP_webpay_Prakticke_scenare_v2.1 GP_webpay_Seznameni_se_systemem_v2.1
1.0	17.06.2016	GPE Product	Document revision
1.1	13.09.2016	GPE Product	Adding „Table No. 2: Periods for payment processing“
1.2	10.10.2016	GPE Product	Updated „Table No. 2: Periods for payment processing“
1.3	18.11.2016	GPE Product	Updated „Table No. 2: Periods for payment processing“
1.4	3.1.2017	GPE Product	Updated „Table No. 2: Periods for payment processing“
1.5	28.12.2018	GPE Product	Document revision, adding newly implemented functionalities
1.6	10.5.2019	GPE Product	Document revision, adding newly implemented functionalities
1.7	30.12.2019	GPE Product	Document revision, adding newly implemented functionalities
1.8	15.05.2020	GPE Product	Document revision, adding newly implemented functionalities
1.9	14.07.2021	GPE Product	Document revision, adding newly implemented functionalities

Table of contents

1. Formula clause 4
2. Introduction 5
3. Process of payment 6
4. Card payment 7
4.1 3D Secure payment 7
5. Payment using a digital wallet 8
5.1 Google Pay 8
5.2 Apple Pay 10
6. Payments with payment button 11
6.1 PLATBA 24 11
7. Payments facilitating functionalities 12
7.1 Card on file 12
7.2 Recurring payment 14
7.2.1 Initial settings 14

7.2.2 Registration payment 15
7.2.3 Recurring payment - subscription 15
7.2.4 Cancellation 16
7.3 Fastpay 16
7.4 PUSH payment 17
8. DCC 19
9. Installment payment 21
10. GP webpay Portal 22
11. Scenarios of payment processing 22

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

The user's guide "GP webpay Payment Gateway" aims at e-commerce merchants (hereinafter referred to as the merchant), who accept payments via GP webpay payment gateway in their e-shops.

The manual describes all the functionalities of the GP webpay payment gateway from the merchant's and his/her customer's perspective.

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

The GP webpay payment gateway enables the merchant to:

- Accept 3D Secure payments – cards issued by Mastercard, Visa, Diners Club and American Express associations
- Accept payments using digital wallet –Google Pay and Apple Pay
- Accept payments using payment button – PLATBA 24 (payment button for clients of Česká spořitelna, a.s.)
- Use functionalities facilitating payments – Card on file for One-click/Usage-based payments, Recurring payment for Usage-based, regular & prepaid subscriptions, Fastpay, PUSH payment
- Payments in the domestic currency of the customer using the DCC service
- Installment payment for all payment cards Mastercard
- Use intuitive and responsive design of payment page
- In cooperation with acquirer use functionalities to limit frauds – Fraud Prevention System
- Use API HTTP and API WS (Web Services) interface for integration with e-shop – see technical specification for developers
- Use the GP webpay Portal – management of payments, users, and keys, download of technical documentation and other sources for integration with GP webpay payment gateway interface, see the user's guide for the GP webpay Portal

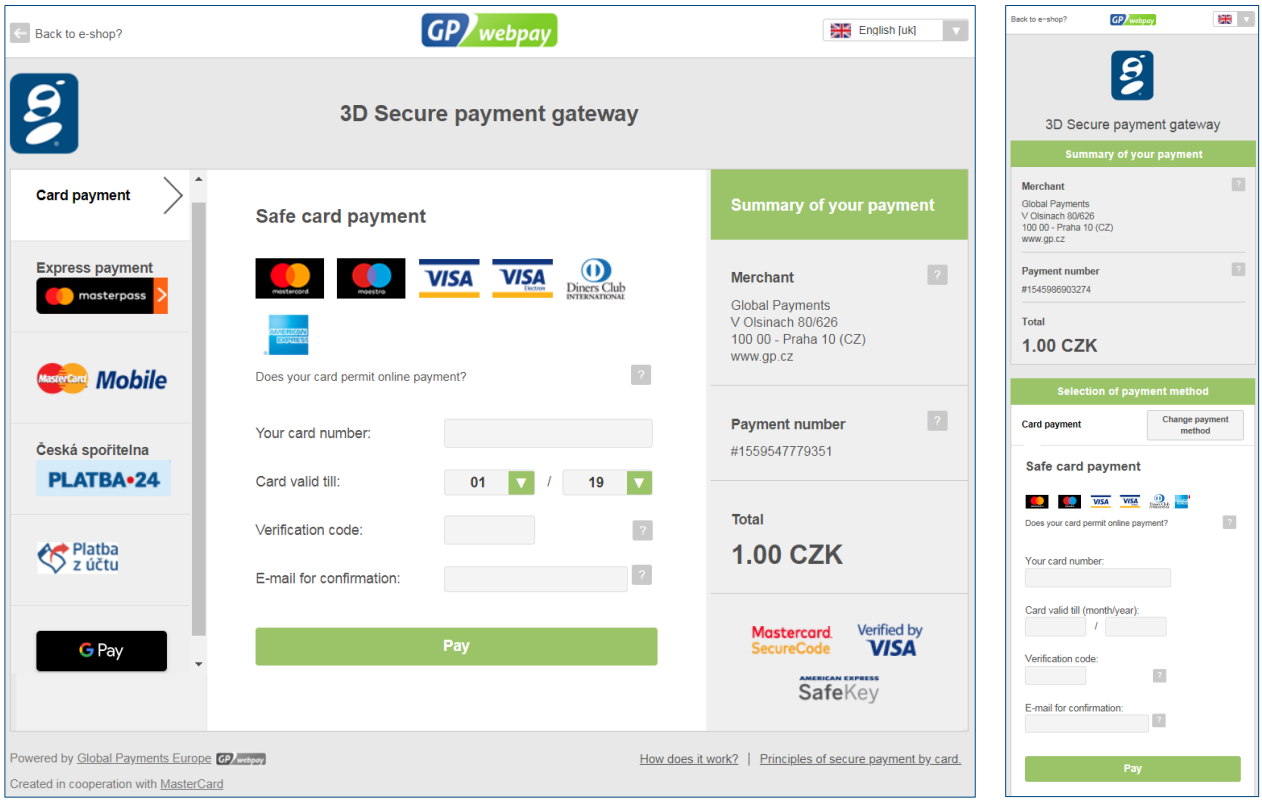
3. Process of payment

When requiring an online payment from a customer, the merchant creates a request to create a payment in his/her e-shop and sends it to the GP webpay payment gateway interface (API) (see technical specification for developers).

After the GP webpay payment gateway receives a request to create a payment, it creates an object named ORDER and redirects the customer's browser to the payment page for payment method selection.

Payment page has responsive design and adjusts automatically to screen of a used device and to browser's language (see Picture No. 1). Customer can change the language of the payment page in the dropdown menu in the upper right corner.

Logo in the upper corner and colour of selected graphical elements (the "Pay" button, the "Summary of your order" and arrows for card validity selection) is displayed according to the acquirer of an e-commerce merchant.



Pic. 1: Display of payment page on a standard PC (desktop) and on mobile device for a GPE merchant

Customer can select a payment method by clicking the relevant button in the left part of the payment page.

If customer decides not to accomplish the payment, he/she can click on the link "Back to e-shop" in the upper left corner.

After payment accomplishment, the GP webpay payment gateway sends a payment result to the merchant (see technical specification for developers).

The GP webpay payment gateway enables recurring entry of the card – the customer has up to 3 attempts at making the payment successfully (authorization). Where the payment is not made, the customer is informed about the most frequent reasons:

- Non-authentication by the 3D Secure system
- Rejection by the issuer bank

The customer is also informed about further steps to make the payment successfully:

- Check the card authorization for payments on the Internet
- Check the card setting for authentication in the 3D Secure system
- Check the sufficient balance on the card account
- Use another card

The payment page contains a field for entering an e-mail address to which the confirmation of blocking of cardholder's funds is to be sent (hereinafter referred to as the "confirmation"). Entering the e-mail address is optional for the customer. Where the customer sends an e-mail address in the EMAIL parameter (API HTTP interface), that e-mail address is displayed – it may be changed or deleted by the customer.

4. Card payment

Customer enters the card number, card validity and verification code, and confirm the request to make the payment by pressing the "Pay" button.

4.1 3D Secure payment

In the case of cards issued by Mastercard, Visa, Diners Club and American Express associations, the payment is under way with 3D Secure defined by card associations under the name Mastercard Identity Check, Visa Secure, Discover ProtectBuy and American Express SafeKey. 3D Secure standard guarantees particularly authentication of a cardholder by a card issuer in the course of payment and provides all the parties (cardholder, card issuer, e-commerce merchant, acquirer bank) with incomparably higher guarantees compared to non-authenticated SSL payments (see Picture No. 2).

Pic. 2: 3D Secure payment

The merchant can allow a customer to carry out a 3D Secure card payment without a redirection to the issuing bank (issuer) and without strong customer authentication provided that the merchant implements and uses the extended parameter of ADDINFO (see the up-to-date version of the document "GP webpay API HTTP – Technical Specification"), in which they provide information required for the Transaction Risk Analysis (TRA) of the given payment.

Providing that, based on a previous agreement between the acquirer and the merchant, the TRA exemption from the strong customer authentication is applied by the acquirer with whom the merchant has concluded an agreement on payment cards acceptance on the Internet, the responsibility for chargebacks is not transferred to the issuer and potential damages are the responsibility of the acquirer, who can transfer this duty to the merchant.

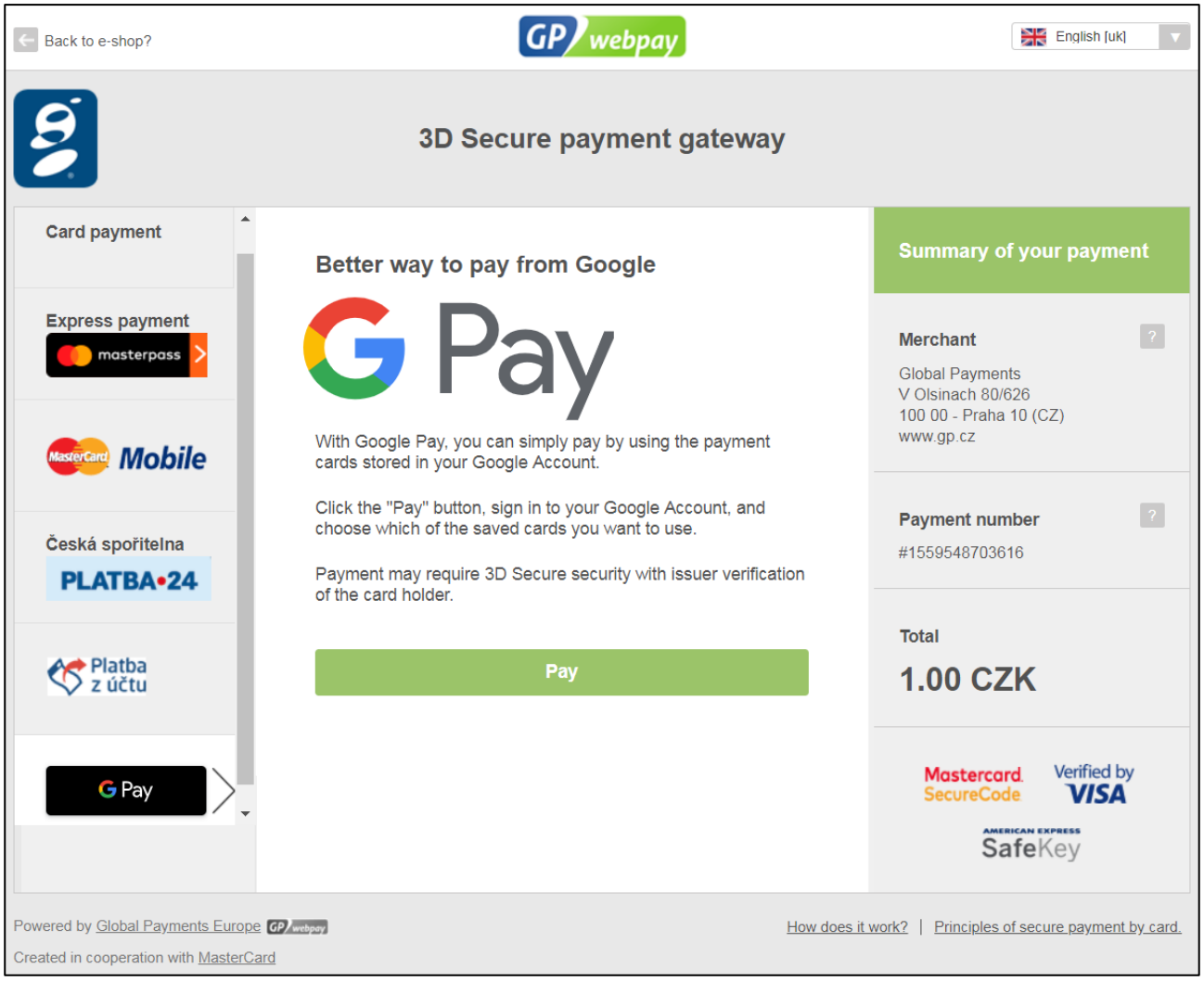
Providing that the TRA exemption from the strong customer authentication is applied by the issuer, the responsibility for chargebacks is transferred to the issuer, who is responsible for potential damages (status quo).

5. Payment using a digital wallet

5.1 Google Pay

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

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 (see Picture No. 3). 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.



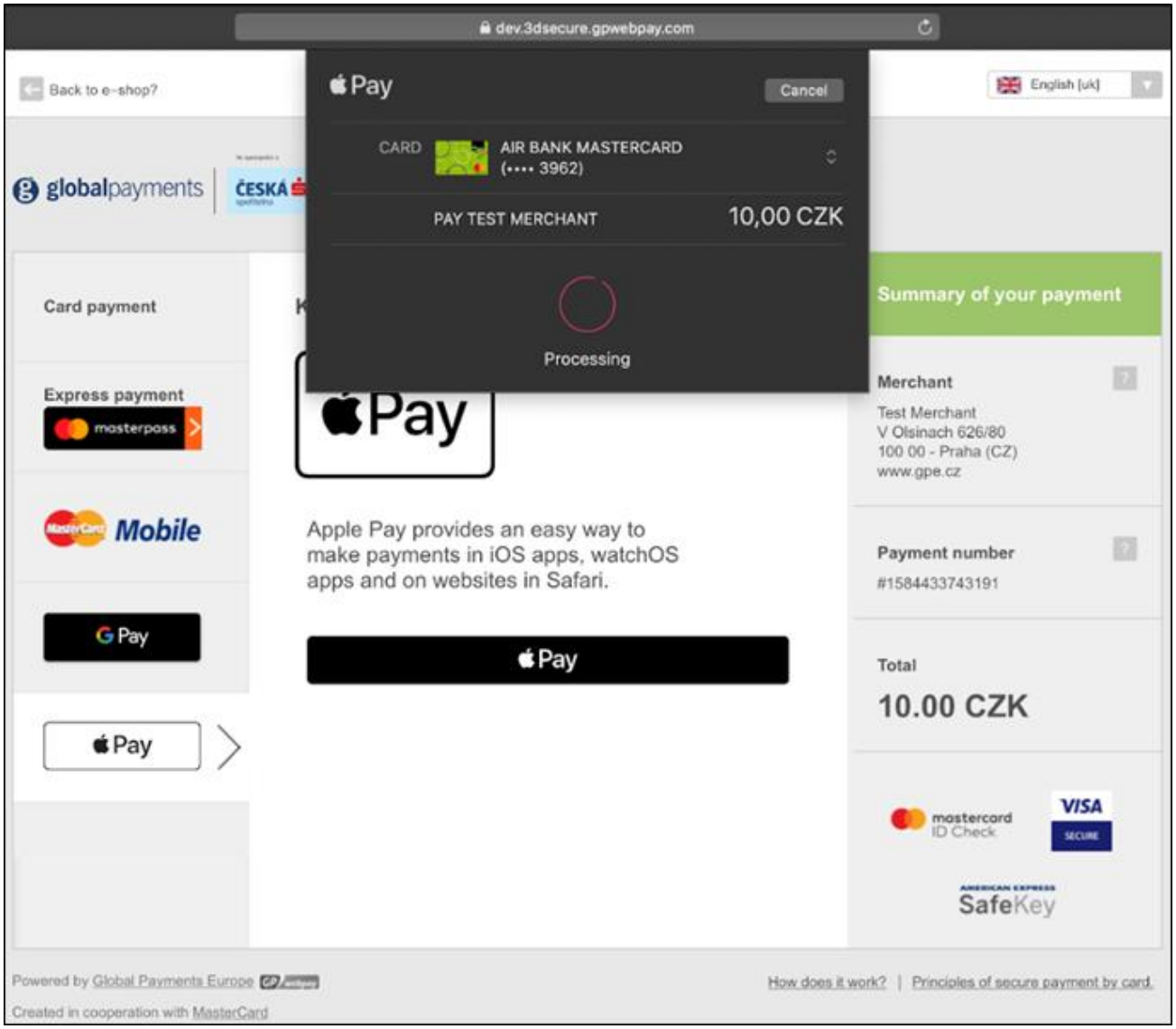
Pic. 3: Page containing information on Google Pay payment for the customer

Google Pay may be offered directly on the web pages of the e-shop by means of the "G Pay" button (see Picture No. 4). For such cases of use, the e-shop integration is described in the technical specification for developers.

Pic. 4: "G Pay" button

5.2 Apple Pay

Apple Pay provides an easy and secure way to pay on iOS, watchOS, and iPadOS devices in the app and Safari browser, and on MacOS devices in Safari browser. Apple Pay uses device specific tokenized credit or debit payment cards (DPAN). When the customer confirms the payment using Face ID, Touch ID or access code, tokenized cards data are processed as standard online card payment (see Picture No. 5).



Pic. 5: Page containing information on Apple Pay payment for the customer

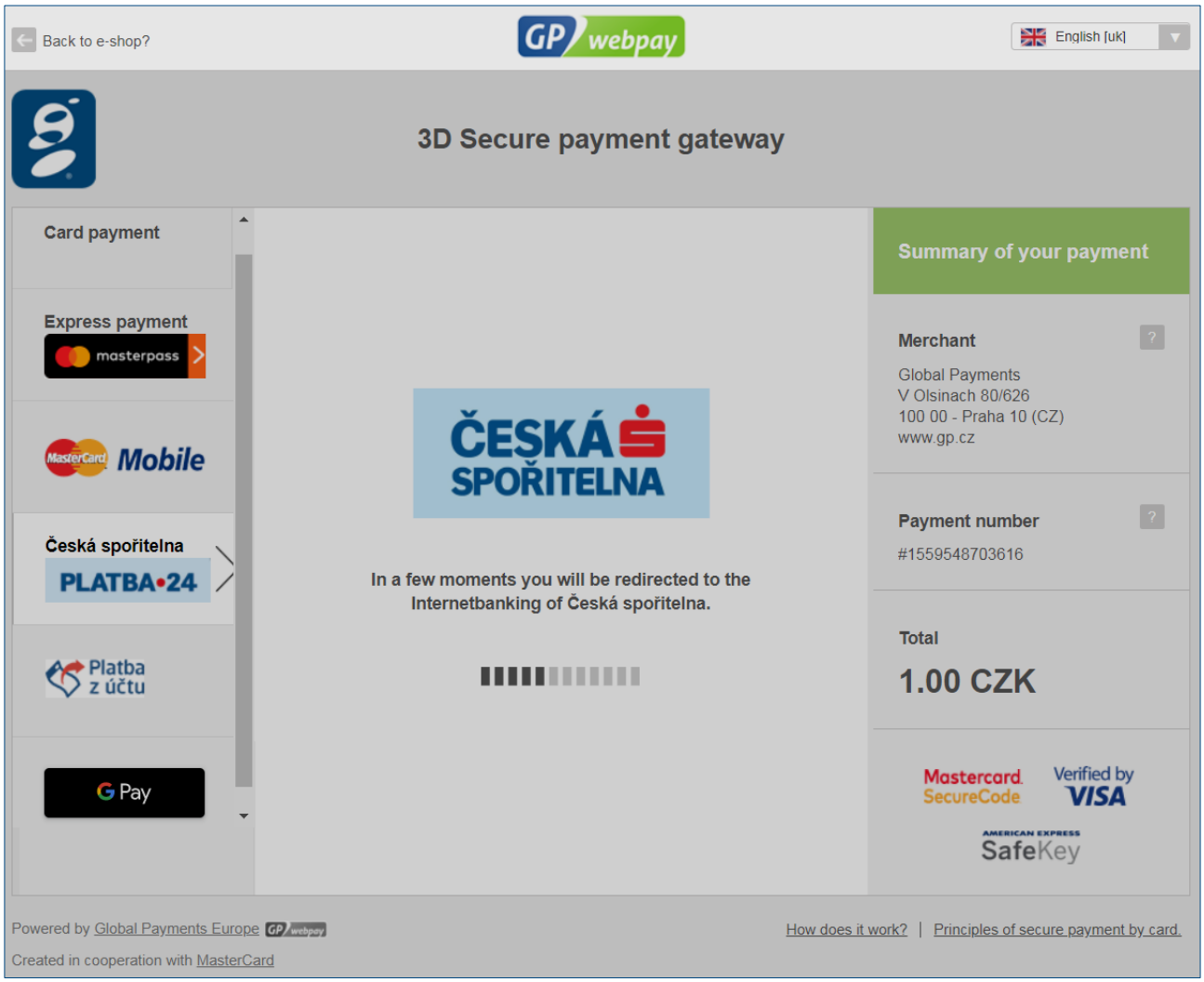
Apple Pay may be offered directly on the web pages of the e-shop by means of the "Apple Pay" button. For such cases of use, the e-shop integration is described in the technical specification for developers.

6. Payments with payment button

6.1 PLATBA 24

PLATBA 24 is a payment button of the SERVIS 24 internet banking provided by Česká spořitelna, a.s.

To make a payment via PLATBA 24, the customer clicks on "PLATBA 24 Česká spořitelna" button and the payment gateway GP webpay redirects the customer´s browser to the login page of Česká spořitelna, a.s. (see Picture No. 6).



Pic. 6: Redirecting of the customer's browser to the Česká spořitelna internet banking

Login page of the of the SERVIS 24 internet banking provided by Česká spořitelna is displayed (see Picture No. 7), where the customer can complete the payment then.

Pic. 7: Login page of the SERVIS 24internet banking provided by Česká spořitelna

PLATBA 24 can be offered directly on the e-shop web pages by means of the "PLATBA 24" button (see Picture No. 8). Integration of the e-shop for this use case is described in the technical specification for developers.

PLATBA 24

Pic. 8: "PLATBA 24" button

7. Payments facilitating functionalities

7.1 Card on file

The Card on file functionality enables the merchant to store, in a simple and secure way, card details in GPE systems (card number and validity) for the purposes of:

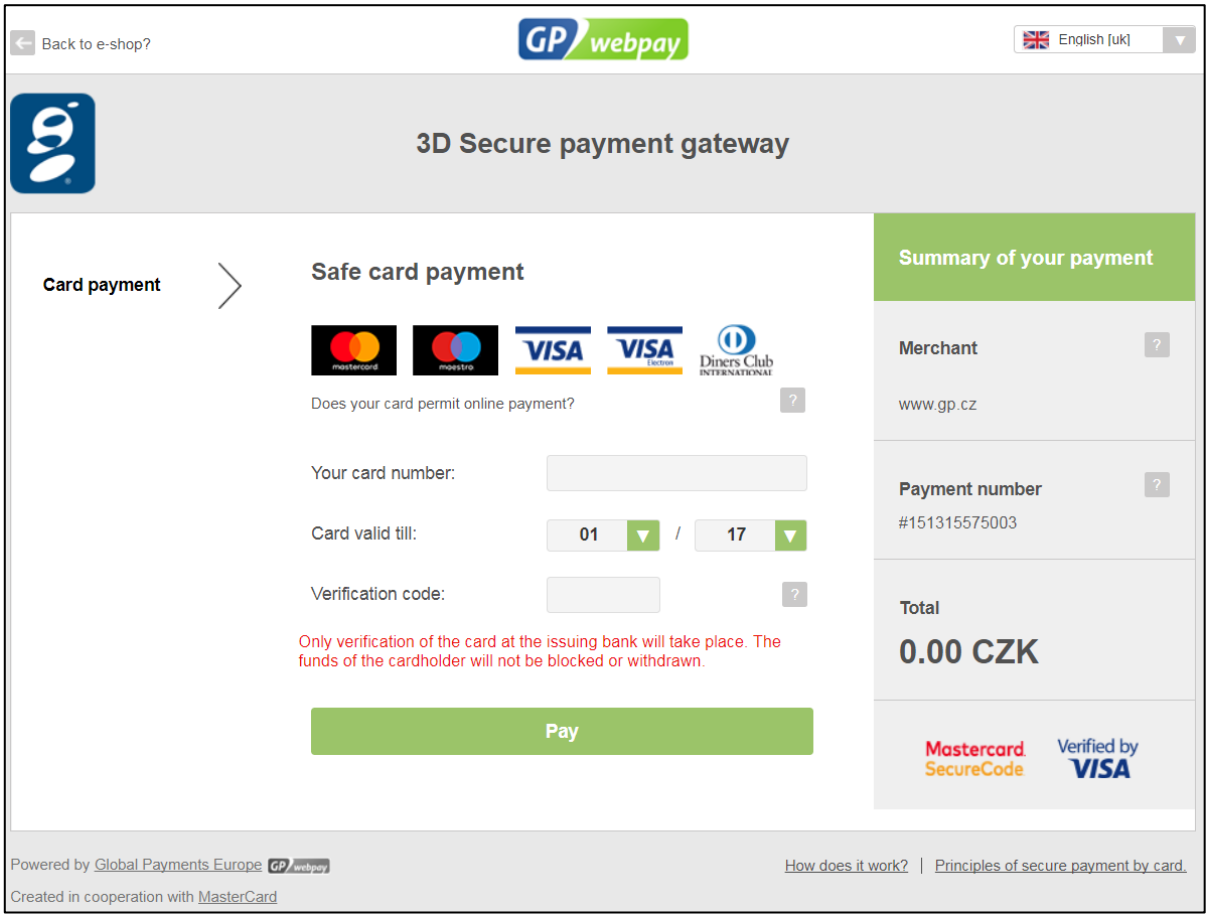
- One-click Payment:

  - A customer clicks the "Pay" button in the e-shop or in the merchant's application and the payment is immediately processed via the GP webpay API WS without redirecting the customer to the GP webpay payment gate.
  - In this case, the merchant shall implement the new method of processCardOnFilePayment (see the up-to-date version of the document "GP webpay API WS – Technical Specification"). API HTTP must also be implemented in case the processCardOnFilePayment method response is with a requirement for redirecting the customer to their issuing bank (issuer) to ensure a strong customer authentication.
  - The acquirer authorises the One-click Payment function for the merchant; this payment does not transfer the responsibility for chargebacks to the issuer and potential damages are the responsibility of the acquirer, who can transfer this duty to the merchant.

- Usage-based Payment:
  - A customer clicks the "Pay" button in the e-shop or in the merchant's application but the payment is initiated by the merchant and processed via the GP webpay API WS later without redirecting the customer to the GP webpay payment gate, take a payment initiated by a transport service application such as Uber as an example.
  - In this case, the merchant shall implement the new method of processUsageBasedPayment (see the up-to-date version of the document "GP webpay API WS – Technical Specification").
  - The acquirer authorises the Usage-based Payment function for the merchant; this payment does not transfer the responsibility for chargebacks to the issuer and potential damages are the responsibility of the acquirer, who can transfer this duty to the merchant.

First, the customer has to give consent to the storage of card details in GPE systems. To store the card details, it is possible to use the so-called registration payment which is made in the same way as a standard 3D Secure payment, or the Card verification functionality.

To use the Card verification functionality, the customer is redirected to the payment page of GP webpay which offers only the payment method "Card payment" in the amount of CZK 0 (see Picture No. 9). It also displays a notice that only the card verification with the issuer bank will be performed and that no funds will be blocked or deducted.



Pic. 9: Display of the payment page for the Card verification functionality

7.2 Recurring payment

The functionality Recurring payment is defined by associations as a card payment associated with recurring billing with predetermined and by the customer pre-agreed conditions, such as a date and / or a fixed amount.

7.2.1 Initial settings

At first, the customer has to agree with the agreement regarding the accomplishment of a recurring payment by the merchant (Recurring Transaction Agreement - RTA). RTA has to specify:

- Amount and date
- If the amount / date is fixed or variable
- Way of communication with the customer

An obligation of the merchant is:

- To confirm the RTA to the customer within two days by the agreed way of communication
- RTA has to be retained over the duration of the agreement and provided at the request of the card issuer (by e-mail or in other electronic format, or in paper form)

7.2.2 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 authenticated in that and the payment has to be made. If the payment is rejected, no other payments can be made under the given RTA and the merchant has to inform the customer.

7.2.3 Recurring payment - subscription

If the merchant offers a free trial period, the customer has to be informed 7 days in advance about the payment to be made at the end of that period.

The recurring payment is made by the use of API WS (Web Services) without redirecting the customer's browser to the payment page for entering payment card data. The GP webpay authorizes directly the payment that is being made secured by SSL without authentication of the cardholder.

The merchant shall notify the customer about the upcoming expiration of his card and shall offer him/her an RTA renewal.

The merchant has to notify the customer at least seven working days before the next recurring payment in agreed way of communication in the following cases:

- It has been more than six months since the last payment
- The free trial period, the initial offer, or promotion action has finished
- In the RTA, there has been changed the amount and/or date given for the recurring payment

7.2.3.1 Usage-based Subscription:

A customer agrees with the merchant on a "direct debit from the payment card" (similar to a direct debit from a bank account), for example, on a regular payment for invoices from a mobile telephone network operator (variable amount/fixed date).

In this case, the merchant shall implement the new method of processUsageBasedSubscriptionPayment (see the up-to-date version of the document "GP webpay API WS – Technical Specification").

The acquirer authorises the Usage-based Subscription for the merchant; this payment does not transfer the responsibility for chargebacks to the issuer and potential damages are the responsibility of the acquirer, who can transfer this duty to the merchant.

7.2.3.2 Regular Subscription:

A customer agrees with the merchant on a regular subscription, e.g. a subscription to digital services such as Netflix (fixed amount/fixed date).

In this case, the merchant shall implement the new method of processRegularSubscriptionPayment (see the up-to-date version of the document "GP webpay API WS – Technical Specification").

The acquirer authorises a Regular Subscription for the merchant; this payment does not transfer the responsibility for chargebacks to the issuer and potential damages are the responsibility of the acquirer, who can transfer this duty to the merchant.

7.2.3.3 Prepaid Subscription:

A customer agrees with the merchant on reloading a prepaid service, e.g. a payment to reload a stored value card of a mobile telephone network operator with a fixed amount initiated by a drop of the stored value below the defined level (fixed amount/variable date).

In this case, the merchant shall implement the new method of processPrepaidPayment (see up-to-date version of the document "GP webpay API WS – Technical Specification").

The acquirer authorises the Prepaid Subscription for the merchant; this payment does not transfer the responsibility for chargebacks to the issuer and potential damages are the responsibility of the acquirer, who can transfer this duty to the merchant.

7.2.4 Cancellation

The merchant has to enable the customer an easy and feasible on-line cancellation of the recurring payment.

Also the customer's card issuer can cancel the recurring payment for the customer. In that case the registration payment is invalidated and no recurring payments can be made to it.

Registration payment is invalidated automatically, if no recurring payment has been created to it over one calendar year, and no recurring payment can be created to it any more.

Creating a registration or recurring payment, it is described in the technical specification for developers.

Important notice: a recurring payment cannot be made for Maestro payment cards.

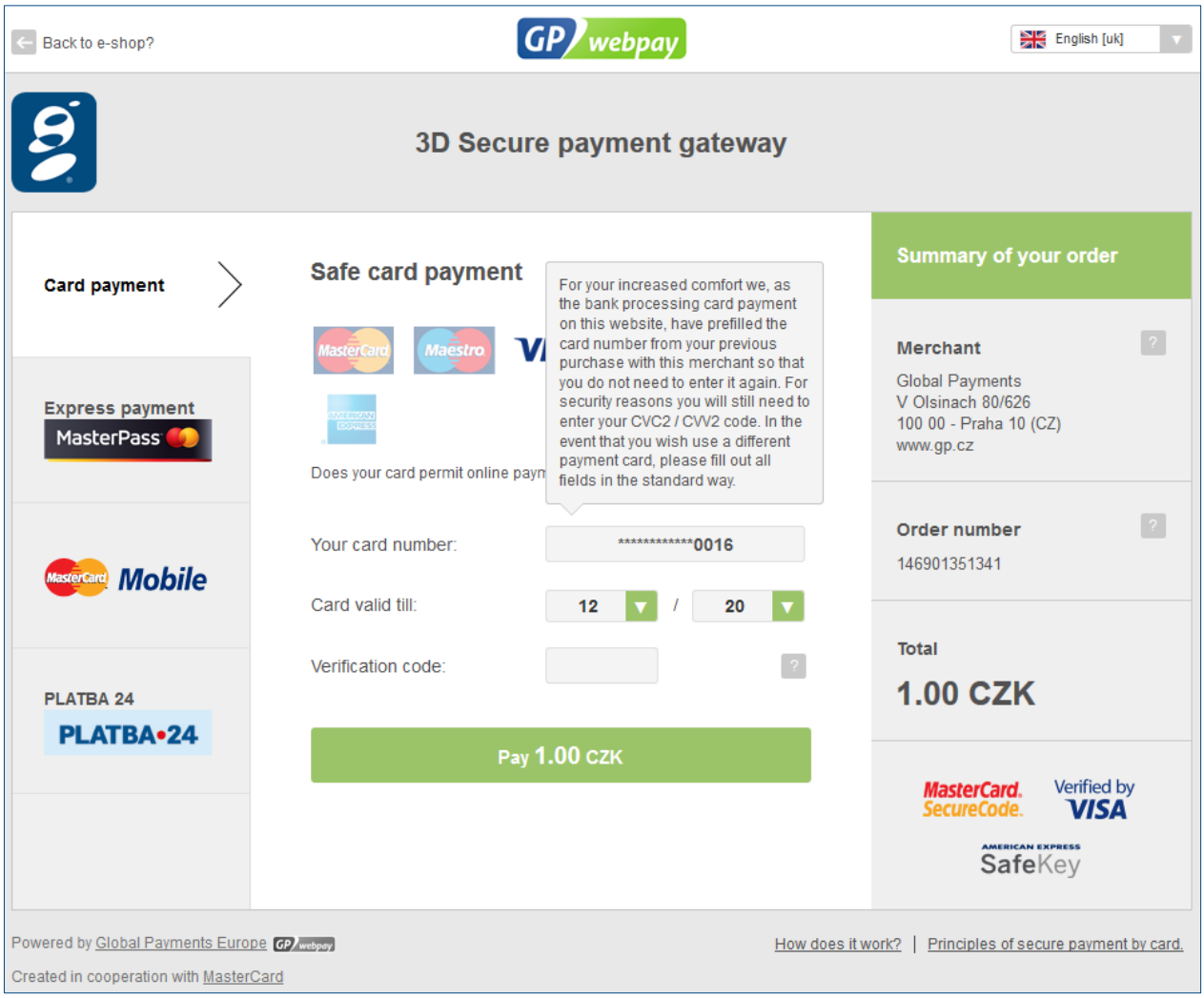
7.3 Fastpay

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 (see Picture No. 10). The customer enters only verification code (CVC2/CVV2), the payment is created as a standard payment 3D Secure with cardholder's authentication.

The merchant shall notify the customer in advance concerning the use of this functionality.

The customer can rewrite the displayed data and pay by other card.

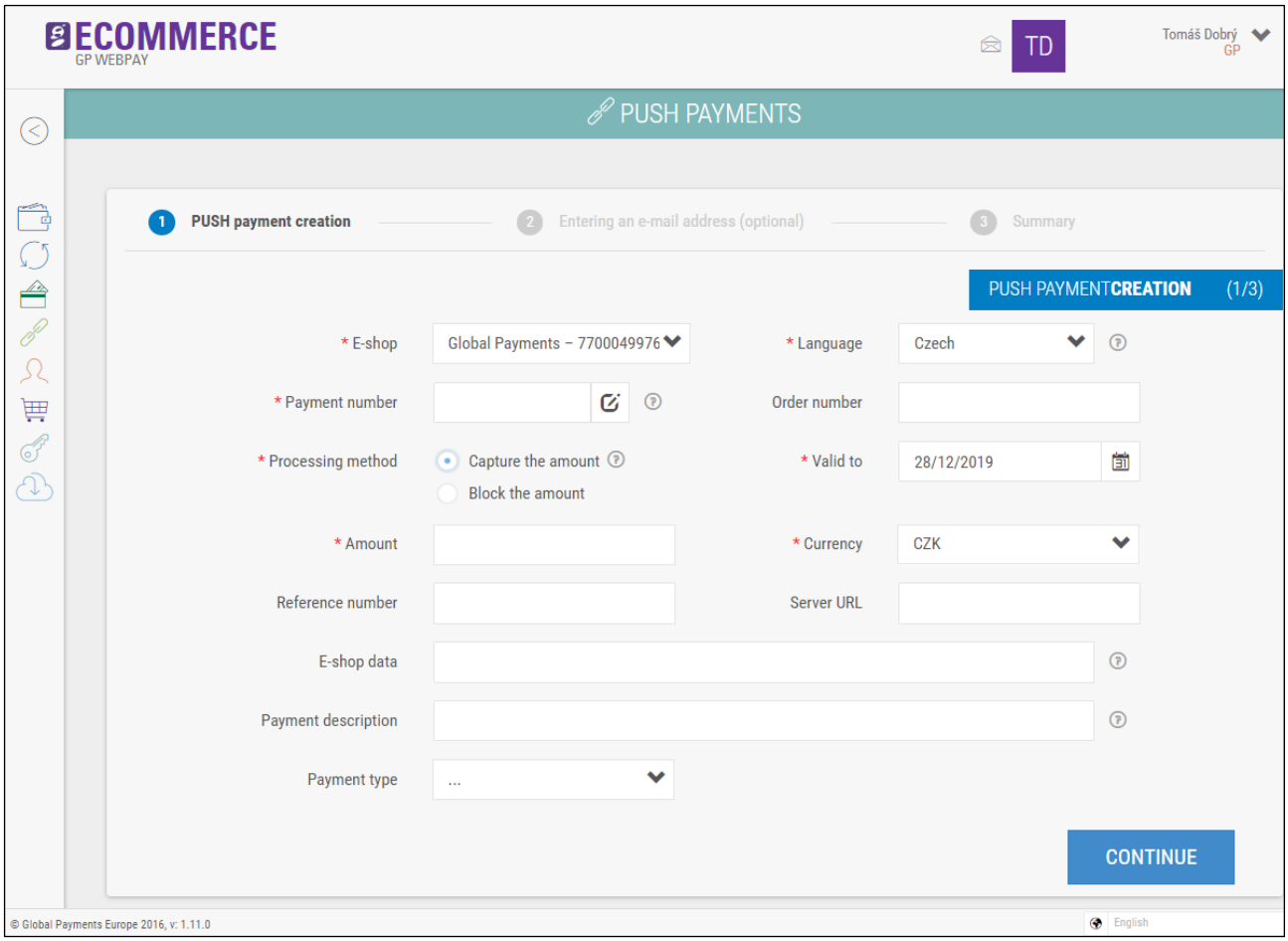
Integration of e-shop to use this functionality is described in the technical specification for developers.



Pic. 10: Display of the last 4 digits and card validity when using the Fastpay functionality

7.4 PUSH payment

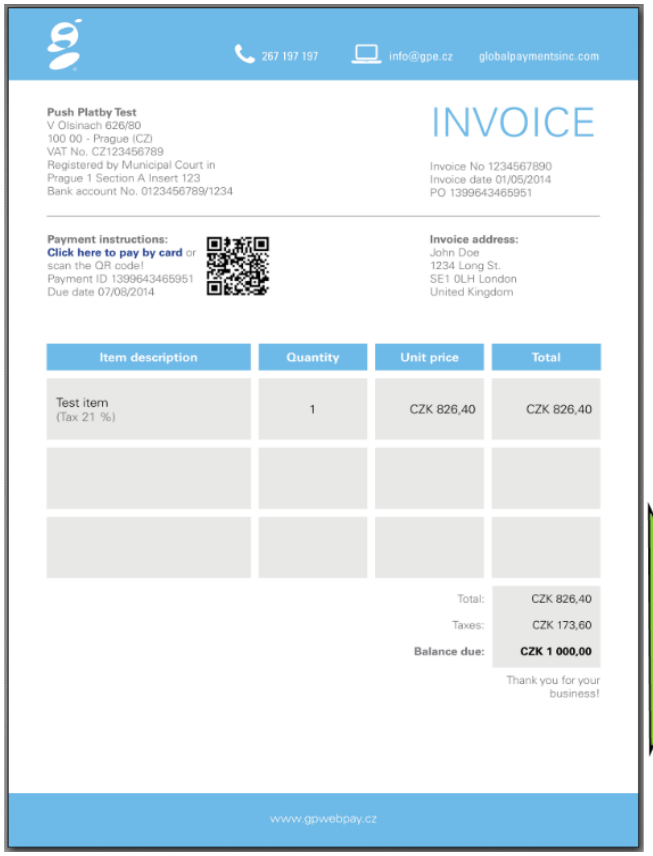
PUSH payment functionality enables the merchant to create a payment request (so-called payment link). The merchant can create a PUSH payment in the GP webpay Portal (see Picture No. 11) or via API WS (see technical specification for developers).



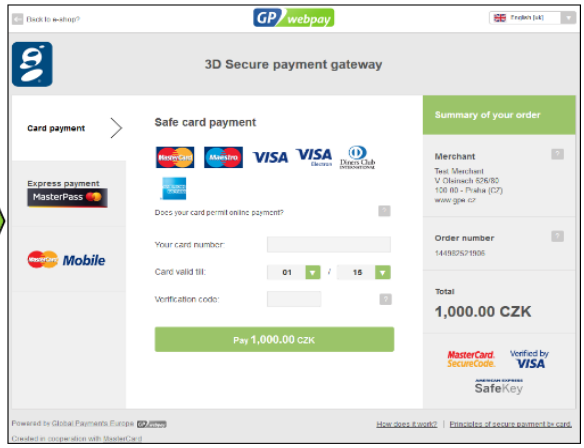
Pic. 11: Creating a PUSH payment in the GP webpay Portal

The payment link can be sent to the customer by e-mail, or a QR code can be generated from it (e.g. to be placed on invoice, see Picture No. 12). If the customer decides to capture the PUSH payment, he/she clicks the link or scan the QR code and his/her browser is redirected to the GP webpay payment gateway, where the payment can be captured as in an e-shop.

The payment link can be used for recurring opening of the payment page and it is possible to make up to three payment attempts.



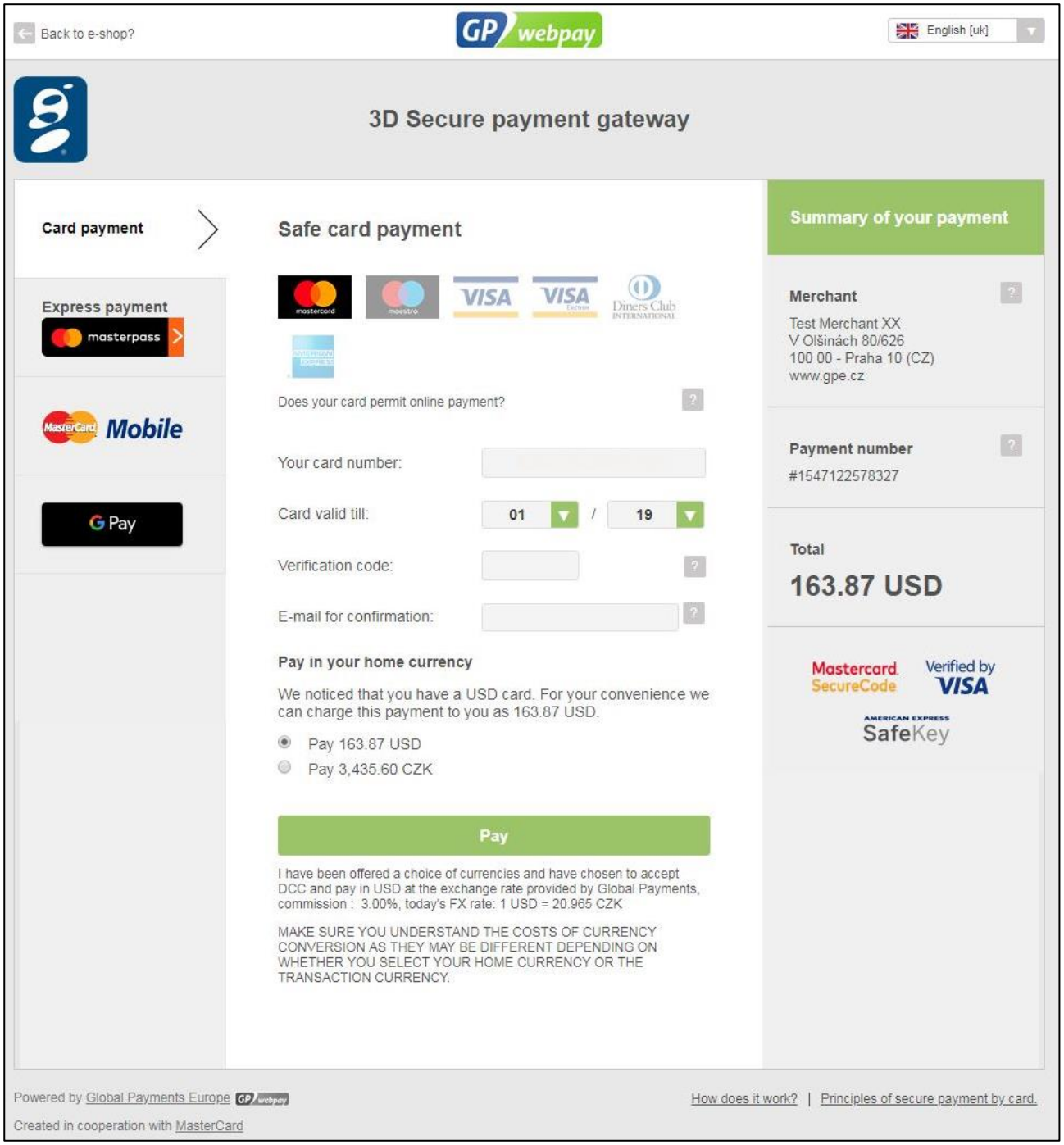
The customer activates the link on the electronic (PDF) invoice or scan QR code on the paper invoice and the internet browser displays the GP webpay payment gateway for card payment of the invoice.



Pic. 12: Using PUSH payment to capture the invoice by card

8. DCC

The DCC (Dynamic Currency Conversion) functionality enables the customer to make payment in his/her domestic currency. The GP webpay payment gate automatically recognizes the domestic currency on the basis of the card number and offers the customer a payment using DCC (see Picture No. 13). Then the customer may choose payment in his/her domestic currency or in the currency of the merchant.



Pic. 13: Display of the payment page including the offer of payment made with the use of DCC

Following the successfully made payment, the GP webpay payment gate displays a confirmation of blocking the funds of the cardholder (hereinafter referred to as the "confirmation"). The confirmation is displayed in a separate "pop-up" window. The same confirmation is also sent to the e-mail address of the customer if he/she entered the address on the payment page. Some browsers may require authorization of the URL address of the GB webpay payment gate for the list of authorized URL addresses in order to display the "pop-up" window.

Customers may pay in various currencies but the settlement is performed as hitherto to the existing account in the domestic currency of the merchant.

DCC may be used without limitation also by merchants accepting foreign currencies. The payment page offering DCC is displayed only for payments in CZK.

9. Installment payment

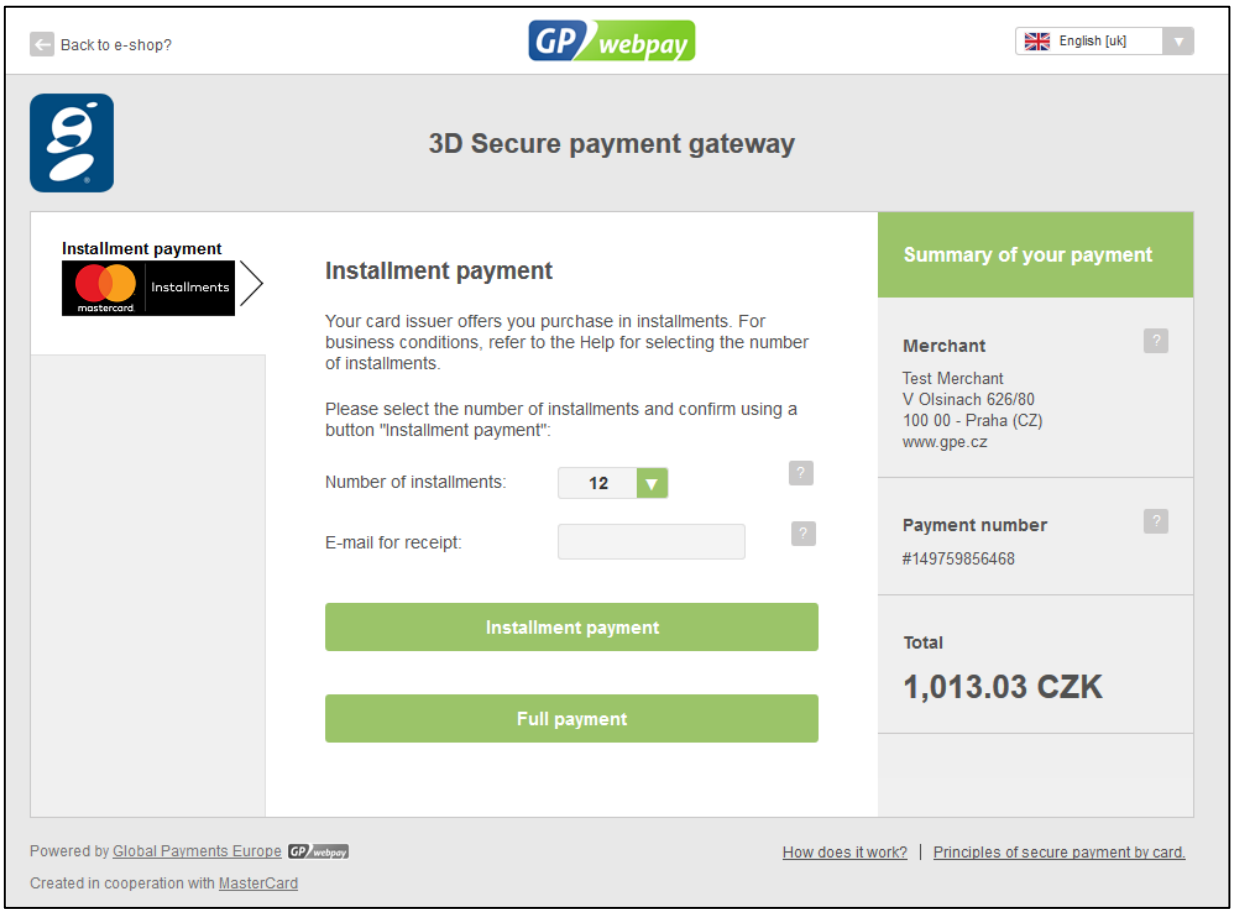
Installment payment functionality enables the customer with payment card Mastercard to pay a purchase from the merchant by installments.

If the customer´s issuing bank is enrolled in the Mastercard program and has agreed the general business terms and conditions with the customer, the payment gateway GP webpay will offer to the customer after successful authorization Installment payment service or to pay a full payment (see Picture No. 14).

In the help window when selecting the number of installments, the card issuer's terms and conditions are displayed. The card issuer has the following options:

- Individual business terms for up to 12 different offers of number of installments (drop-down list)
- Same business terms for a range with minimum and maximum number of installments (drop-down list)
- Business terms agreed in advance (only announcement „According to issuer´s conditions")

Customers can make installment payment or to pay a full payment, but the settlement of these payments towards the merchant is performed as hitherto in full.



Pic. 14: Display of the payment page including the offer of payment made with the use of Installment payment

10. GP webpay Portal

The GP webpay Portal enables the merchant's user (see the "GP webpay Portal" manual) to:

- search and manage payments
- create, send, search and manage PUSH payments
- create and manage users
- display statistics and functionalities authorized for the e-shop and payments
- create and manage keys
- download technical documentation and other sources for integration with the GP webpay payment gateway interface

Some other functionalities of the GP webpay Portal can be used also via API WS (see technical specification for developers) and this way they can be integrated into the merchant's e-shop.

11. Scenarios of payment processing

The GP webpay payment gateway enables the merchant various possibilities of payment processing. The most frequent scenarios of payment processing are described in Table No. 1, for further information, please, see the technical specification for developers and the user's guide "GP webpay Portal". Possible statuses of payment and the main transitions between them are showed in the Picture No. 15.

Scenario	Description	API HTTP	API WS	GP webpay Portal
Payment authorization	The merchant sells goods or services, which are not immediately to dispatch. At the time of receipt of an order from a customer, the merchant requires the payment to be authorized by the issuer bank (authorization) and the amount paid to be blocked on the customer's account. **Important notice:** on the grounds of rules of card associations and according to the agreements with individual acquirers, authorisations are cancelled automatically after expiration of the period given in the Table	The merchant sends the parameter DEPOSITFLAG = 0 in the request to create payment.	The merchant can verify the payment status using the method getOrderState(). Payment status is definitive after 60 minutes after redirecting the customer to the GP webpay payment gateway.	The merchant can verify the payment status in the Payments menu. Payment status can be definitive after 60 minutes after redirecting the customer to the GP webpay payment gateway.

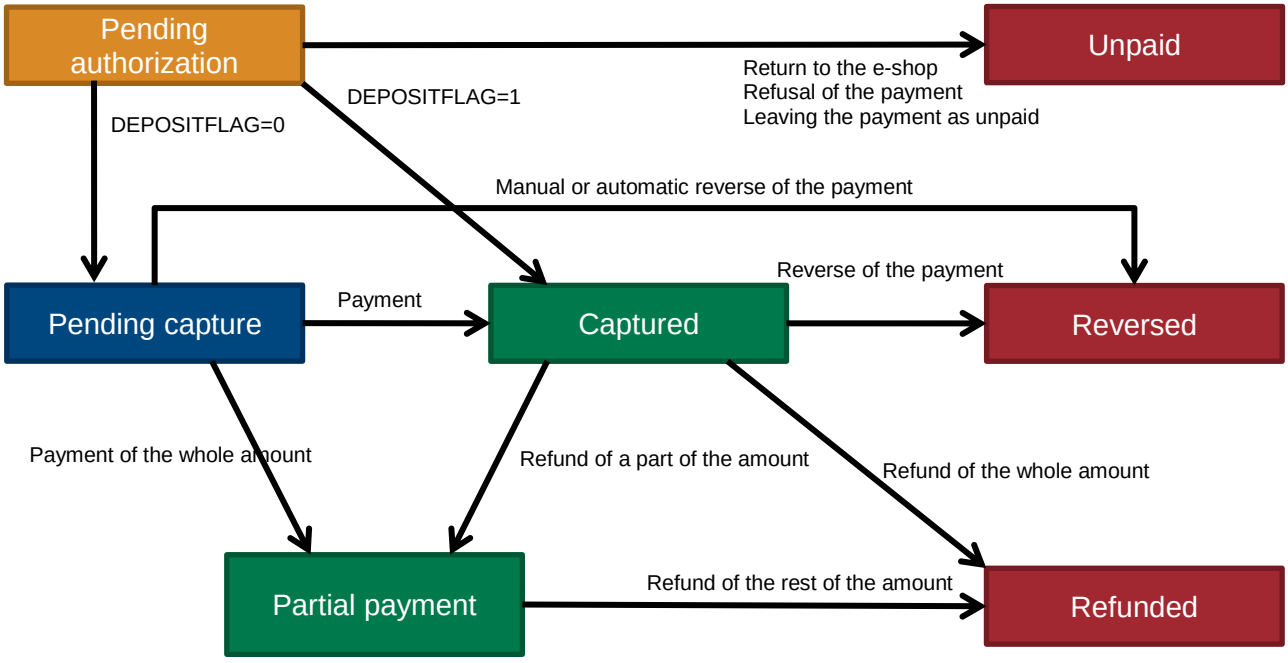
	No. 2. After the given period expires, there will be no possibility to make the scenario "Payment capture".			
Payment capture	The merchant sells goods or services, which are immediately to dispatch. At the time of receipt of an order from the customer, the merchant requires the payment to be authorized by the issuer bank and the amount paid to be captured from the customer's account.	The merchant sends the parameter DEPOSITFLAG = 1 in the request to create payment.	The merchant can verify the payment status using the method getOrderState(). Payment status is definitive after 60 minutes after redirecting the customer to the GP webpay payment gateway.	The merchant can verify the payment status in the Payments menu. Payment status is definitive after 60 minutes after redirecting the customer to the GP webpay payment gateway.
	The merchant has made the scenario "Payment authorization". At the time of delivery of goods to the customer, the merchant requires the blocked amount to be captured from the customer's account.	-	The merchant captures the payment using the method processDeposit().	The merchant captures the payment in the Payments menu.
Payment refund	The customer complains successfully about goods or services and requires the merchant to make full or partial refund. **Important notice:** according to the agreements with individual acquirers, payments are closed automatically after expiration of the period given in the Table No 2. After the given period expires, there will be no possibility to make the scenario "Payment refund". However the merchant can use other method of payment refund (e.g. bank transfer).	-	The merchant refunds the payment using the method processCredit(). For one payment, there can be made more refunds; however the sums of returned amounts must not exceed the originally paid amount.	The merchant refunds the payment in the Payments menu. For one payment, there can be made more refunds; however the sums of returned amounts must not exceed the originally paid amount.
Payment reversal	The merchant has created an incorrect payment and requires cancelling it.	-	The merchant makes payment cancellation using the method	The merchant cancels the payment in the

			processDepositReverse(). **<u>Important notice:</u>** payment cancellation is possible only by payment created with parameter DEPOSITFLAG = 0 and capture of which from the customer's account has not been made yet.	Payments menu. Payment cancellation is possible only for payment created with parameter DEPOSITFLAG = 0 and capture of which from the customer's account has not been made yet.

Table No. 1: The most frequent scenarios of payment processing

Acquirer	Period for automatic cancelling the authorisation	Period for automatic closing the payment
Global Payments s.r.o.	7 calendar days	13 months
Global Payments Europe, s.r.o.	7 calendar days	13 months
Československá obchodní banka, a.s.	7 calendar days	6 months
Československá obchodná banka, a.s.	7 calendar days	6 months
Cataps, s.r.o. (KB SmartPay)	7 calendar days	6 months
EVO Payments International s.r.o. (REVO)	7 calendar days	6 months
UniCredit Bank Czech Republic and Slovakia, a.s.	7 calendar days	13 months

Table No. 2: Periods for payment processing



Pic. 15: Possible statuses of payment and the main transitions between them