July 2023

# METHOD AND SYSTEM FOR PROVIDING DELEGATED ACCESS FOR PROCESSING PAYMENTS USING A PAYMENT GATEWAY

GURPREET BHASIN

# “METHOD AND SYSTEM FOR PROVIDING DELEGATED ACCESS FOR PROCESSING PAYMENTS USING A PAYMENT GATEWAY”

# VISA

**INVENTORS:**

**GURPREET BHASIN**

## TECHNICAL FIELD

[0001] The present subject matter is, in general, relates to processing payments using a Payment gateway, and particularly, relates to a method and system for providing delegated access for processing payments using the Payment gateway.

## BACKGROUND

[0002] Generally, merchants or any business organization typically engage an intermediary party (such as Salesforce or shopping carts) to process payments using payment service provider such as CyberSource. During the process, the business organization (BO) must share BO's credentials with the intermediary party which can be hacked and exposed to malicious users or attackers. For example, if the BO needs to process payments through the payment service provider or a payment gateway (PG) using a Payment Plugin Provider (PPP), and BO has registered with the PG, the PG may grant crypto keys to authorize the BO for enabling the PPP to make the payment on behalf of BO. However, with the BO sharing the crypto keys with the PPP, it may be possible for a hacker to gain access to the crypto keys and makes the payment processing more insecure. Further, to make the payment, the PPP requires implementation of standard protocols like Open Authorization (OAuth) or OAuth2.0 with the PG so as to authorize the PPP and proceed with the payment process. However, typically the PPP does not implement the OAuth or OAuth2.0 as these protocols need User Interface (UI) integration and backend integration with the PG, which consumes more computing resources and additional time. Also, as the OAuth and OAuth2.0 are chatty protocols, they require the tokens to be refreshed frequently which also delay the payment processing and increases the turnaround time of completing the payment processing.

[0003] Thus, there exists a need to address the above disadvantages and provide an efficient, secure, and simple way of providing delegated access to the PPP to enable faster and efficient payment processing to the PG.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0004] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system

and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

[0005] **Fig. 1** illustrates an exemplary architecture block diagram of system for performing an efficient and simpler OAuth for delegated access that implements embodiments consistent with the present disclosure;

[0006] **Fig. 2** illustrates an exemplary process flow diagram that implements embodiments consistent with the present disclosure; and

[0007] **Fig. 3** shows a flowchart diagram illustrating a method for implementing simpler OAuth for delegated access according to embodiments consistent with the present disclosure.

[0008] The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

## DESCRIPTION OF THE DISCLOSURE

[0009] It is to be understood that the present disclosure may assume various alternative variations and step sequences, except where expressly specified to the contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings and described in the following specification are simply exemplary and non-limiting embodiments or aspects. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0010] In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

[0011] While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all

modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

[0012] The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0013] The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

[0014] The terms "including", "comprising", “having” and variations thereof mean "including but not limited to" unless expressly specified otherwise.

[0015] The present disclosure relates to a method and system for enabling merchants (such as a business organization) to grant an authority to an intermediary party such as web based plug in/Payment Plugin Provider (PPP) to make payment or transactions on behalf of the merchants in a secure and efficient manner. To perform the transactions, a payment service provider (such as Payment Gateway (PG)) may create a service that allows the intermediary party to initiate a request with payload for example, unique information of the merchant and claim that the intermediary party has secured authorization on behalf of the merchant. The payment gateway may be previously registered with the merchant and therefore the payload or unique information of the merchant may be available with the payment gateway. Upon receiving the request from the intermediary party, the payment gateway may transmit a request to the merchant to verify the unique information of the merchant. The merchant may verify the unique information and respond to the payment gateway acknowledging the grant of delegated authority to the intermediary party to process the payment or transactions on behalf of the merchant utilizing the payment gateway. Thereafter, the payment gateway initiates a call back request to the intermediary party and transmits a token or transaction key to the intermediary party. The intermediary party uses the received token to make payments on behalf of the

merchant. In this manner, the present disclosure allows the intermediary party to claim a delegated authority to make payments or transactions with increased security and easy adoption by the merchants (one clicks with SMS and or email). In addition, the proposed method and system avoids the need to refresh the OAuth2 token, hence making the process more secure. A detailed explanation is provided below.

[0016] **Fig. 1** illustrates an exemplary architecture block diagram of system **100** for performing an efficient and simpler OAuth for delegated access that implements embodiments consistent with the present disclosure. The system **100** may comprise a merchant device **101**, a Payment Plugin Provider **103** and a Payment Gateway (PG) **105** communicatively coupled via at least one communication network (not shown). The merchant device **101** may be associated with a merchant including, but not limited to business organizations, etc., In some embodiments, the merchant device **101** may include a computing device such as a laptop, a personal computer (PC), mobile device, tablet, etc., that is capable of enabling the merchant to initiate payment processing.

[0017] In some embodiments, the merchant device **101** may be configured to process payments or transactions through the PG **105**. The PG **105** may include, but not limited to, PayPal, RazorPay, CyberSource etc., In some embodiments, the merchant device **101** may communicate with the PG **105** via a payment network (not shown) such as Visa® card network. In some embodiments, the payment network may include the PPP **103** that acts as an intermediary party between the merchant device **101** and the PG **105**. In a non-limiting embodiment, the PPP **103** may be connected to the merchant device **101** and the payment gateway **105** via the Visa card network. For example, the PPP **103** may provide a web based payment plugin such as Salesforce or shopping carts etc.,

[0018] In operation, the merchant may request the PPP **103** to make a payment utilizing the PG **105**. PG **105** may be configured to create a web service that may allow the PPP **103** or any intermediary party to send a request via the web service to the PG **105** for processing the payment request from the merchant. In one example, the request may include a payload of the merchant such as profile information and declaration that the PPP **103** has secured authorization on behalf of the merchant to make the payment. Upon receiving the request, the PG **105** may verify the authenticity of the PPP **103** based on the payload information of the merchant sent via the request. In some embodiments, the PG **105** may be pre-registered with

the merchant and therefore, the payload information such as profile information including contact details may be already available to the PG **105**. The contact details may include at least one of: a mobile phone number, an email address of the merchant or any other equivalent identity of the merchant. The PG **105** validates the payload information based on the profile information previously stored with the PG **105** and upon validation, the PG **105** transmits a request for acknowledgement of the delegated authorization provided to the PPP **103** by the merchant for processing the payment transaction. The PG **105** transmits the request to the merchant identified by the registered contact details such as mobile phone number or the email address respectively. The acknowledgement request may be sent as, for example, a Short Message Service (SMS) message, or a WhatsApp® message, etc., The merchant device **101** receives the acknowledgement request and transmits a confirmation to the PG **105** affirming the delegated authorization to the PPP **103** for making the payment processing on the behalf of the merchant by utilizing the PG **105**.

[0019] Upon receiving the confirmation from the merchant device **101**, the PG **105** makes a web-based call back request to the PPP **103** and generates an encryption key which can be used to confirm the payment transaction. In some embodiments, the encryption key may be, but not limited to, a symmetric crypto key. In a non-limiting embodiment, the PG **105** may implement Public Key Infrastructure (PKI) based mechanism, where the PG **105** may generate a private key and public key, and only share public key with the PPP **103**. In some embodiments, the PG **105** may create and transmit asymmetric keys for delegated access to the PPP **103**. Upon generating the encryption key, the PG **105** transmits the encryption key to the PPP **103** via the payment network. In an embodiment, the PPP **103** uses the received encryption key to make payments on behalf of the merchant.

[0020] In non-limiting embodiment, in case of multiple distinct merchants utilizing the same PPP **103**, the PG **105** may be configured to transmit different acknowledgment requests to confirm the delegated authorization of the PPP **103** to process payments on behalf of the merchants via the PG **105** Post confirmation, the PG **105** may be configured to transmit different encryption or crypto keys to the PPP **103** to be uniquely used for the multiple distinct merchants. By way of verifying the delegated authorization to the PPP **103** before sharing the encryption key with the PPP **103**, the present disclosure enhances the security in payment processing. Further, the present disclosure eliminates the need for the PPP 103 to utilize the chatty protocols thereby avoiding the need to refresh the OAuth token frequently. Further, the

present disclosure dispenses the need to send a crypto key frequently by providing the symmetric key to the PPP **103** that can be used to generate a new token for each payment request. Thus, the present disclosure provides an efficient, reliable and simpler OAuth for delegated access to process the transactions/payments.

[0021] **Fig. 2** illustrates an exemplary an exemplary process flow diagram **200** that implements the system **100** and other embodiments consistent with the present disclosure. As illustrated in the Fig. 2, at step 1, the BO **101** logs into the PPP **103** and requests the PPP **103** to make payment using the PG **105**. At step 2, the PPP **103** generates and transmits a web service call to the PG **105** by transmitting a unique identifier or payload for the given BO **101**. The PG **105** at step 3, transmits a message to the BO **101** via either an email or mobile phone for requesting to make choices of delegation capabilities requested by PPP **103**. At step 4, the BO **101** confirms the PG **105** on the delegation capabilities to be granted to PPP **103** on behalf of the BO **101**. The PG **105** at step 5, creates roles of PPP **103** for distinct BOs and delegation capabilities granted to the PPP **103** and creates a symmetric key for each of the BOs. In some embodiments, the roles and delegation capabilities granted to the PPP **103** may be stored in a database (not shown) associated with the PG **105**. At step 6, the PG **105** invokes the webhook call and transmits the symmetric key to the PPP **103**, thereby allowing the PPP **103** to process payments on behalf of the BO **101**. At step 7, the PPP **103** makes payment and other transactions using the same symmetric key.

[0022] **Fig. 3** shows a flowchart illustrating a method **300** for providing an efficient and simpler OAuth delegated access in a secure way according to embodiments consistent with the present disclosure.

[0023] The method **300** of providing the efficient and simpler OAuth delegated access includes interaction between a merchant device **101**, a payment plugin provider **103** and a payment gateway **105** hosted on a payment server via at least one communication network.

[0024] In an embodiment, the method **300** at block **301** comprises receiving, by a payment gateway (PG) **105**, a request comprising a payload and indicating an authorization for processing transactions on behalf of a merchant associated with the merchant device **101**.

[0025] The method **300** at block **303** comprises transmitting, by the PG **105**, an acknowledgment request to registered contact details of the merchant device **101**. The acknowledgement request may comprise a request to approve or grant authorization to the PPP **103** for processing the transactions on behalf of the merchant.

[0026] The method **300** at block **305** comprises receiving a confirmation of authorization of the PPP **103** in response to the acknowledgement request. Post confirmation, at block **307**, the method **300** may comprise transmitting an encryption key to the PPP **103** to process the transactions on behalf of the merchant.

[0027] The present disclosure offers significant technical benefits such as increase in reliability by reducing the chattiness between the PPP **103** and the PG **105**. Further, since the encryption key may include symmetric or asymmetric key replacing the plaintext access code, the need to refresh the access code frequently do not arise. In addition, the present disclosure enhances security by sharing the symmetric key only once between the PPP **103** and the PG **105,** whereas conventionally the access code is required to be transmitted every time the transaction being performed. Further, the present disclosure does not allow the PPP **103** to obtain the BO **101** login credentials by restricting the illegit or malicious PPP from creating a fake replica of genuine PG **105**, thereby increasing the security. In addition, the present disclosure enhances the user efficiency by now allowing any BO **101** to log into the PG **105** website, since the BO **101** receives the acknowledgment request to grant and authorize the PPP **103** to process transaction on its behalf.

[0028] In an embodiment, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. A non-transitory computer readable medium may include media such as magnetic storage medium, optical storage, volatile and non-volatile memory devices etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic

(e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

[0029] The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor may read and execute the code from the computer readable medium. The processor is at least one of a microprocessor and a processor capable of processing and executing the queries.

[0030] The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building steps have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items or meant to be limited to only the listed item or items. It must also be noted that as used herein, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

[0031] Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural

as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

# “METHOD AND SYSTEM FOR PROVIDING DELEGATED ACCESS FOR PROCESSING PAYMENTS USING A PAYMENT GATEWAY”

## ABSTRACT

The present disclosure relates to a method and system for providing an efficient and simpler OAuth for delegated access in a secure way. The method comprises receiving, by a payment gateway (PG) **105**, a request comprising a payload and an indication of authorization for processing transactions on behalf of a merchant associated with the merchant device **101**. The method comprises transmitting, by the PG **105**, an acknowledgment request to registered contact details of the merchant device **101**. The acknowledgement request may comprise a request to approve or grant authorization to the PPP **103** for processing the transactions on behalf of the merchant. The contact details may comprise at least one of: a mobile phone number or email address of the merchant. The method comprises receiving a confirmation to authorize the PPP **103** in response to the acknowledgement request. Post confirmation, method may comprise transmitting an encryption key to the PPP **103** to process the transactions on behalf of the merchant.

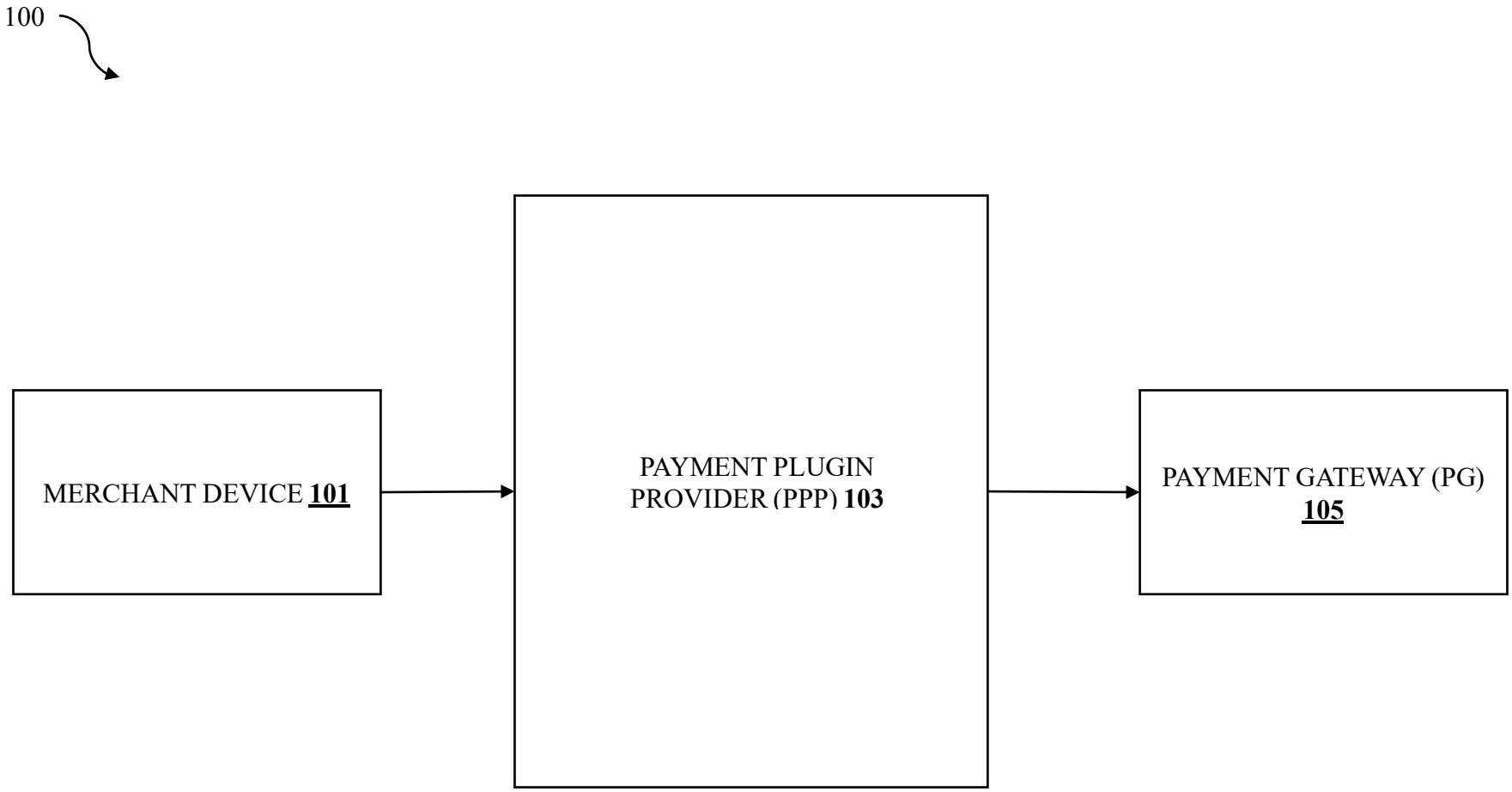
100
MERCHANT DEVICE **101**
PAYMENT PLUGIN PROVIDER (PPP) **103**
PAYMENT GATEWAY (PG) **105**

**Fig. 1**

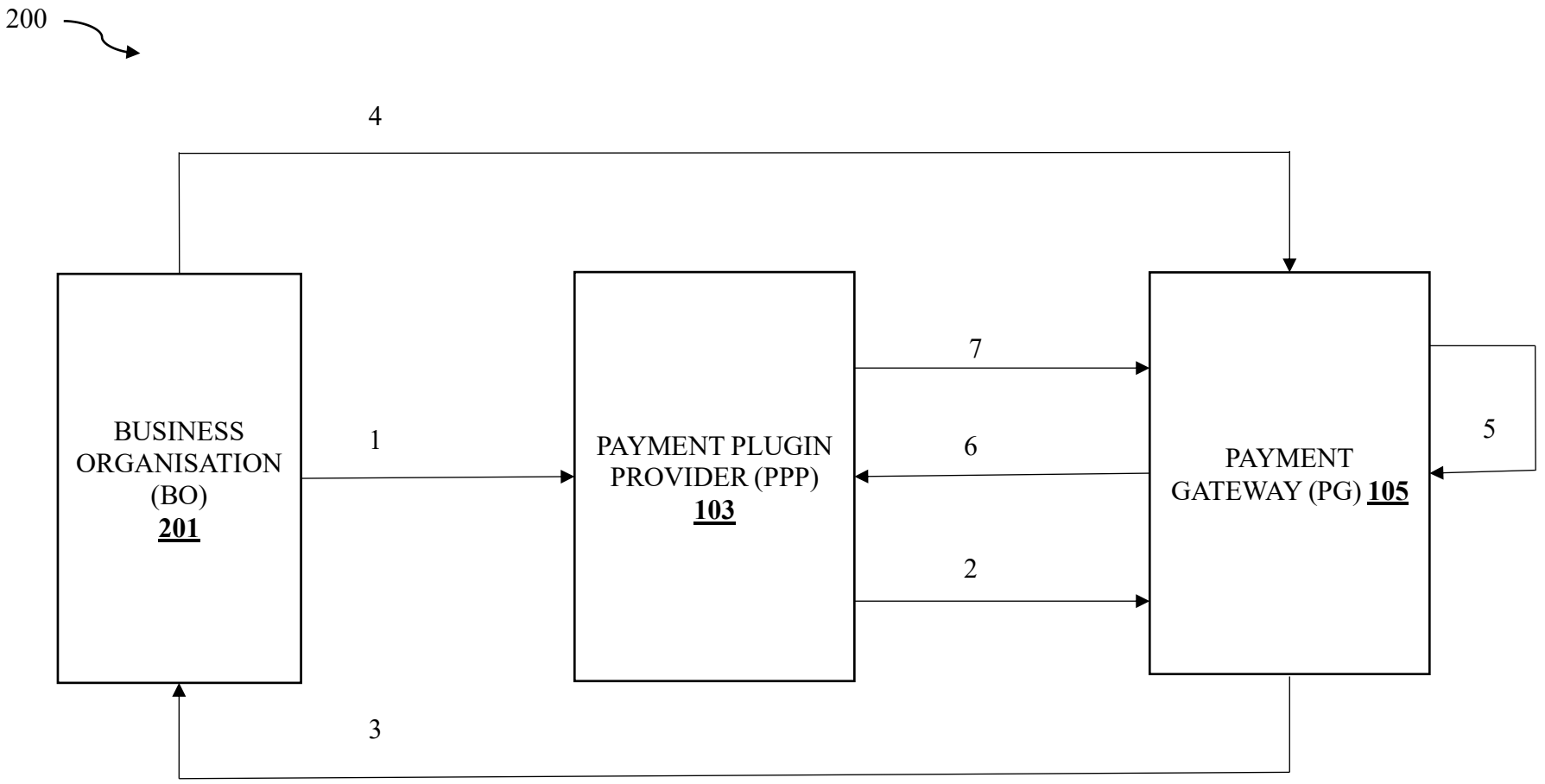
200
4
BUSINESS ORGANISATION (BO) 201
1
PAYMENT PLUGIN PROVIDER (PPP) 103
7
6
2
PAYMENT GATEWAY (PG) 105
5
3

**Fig. 2**

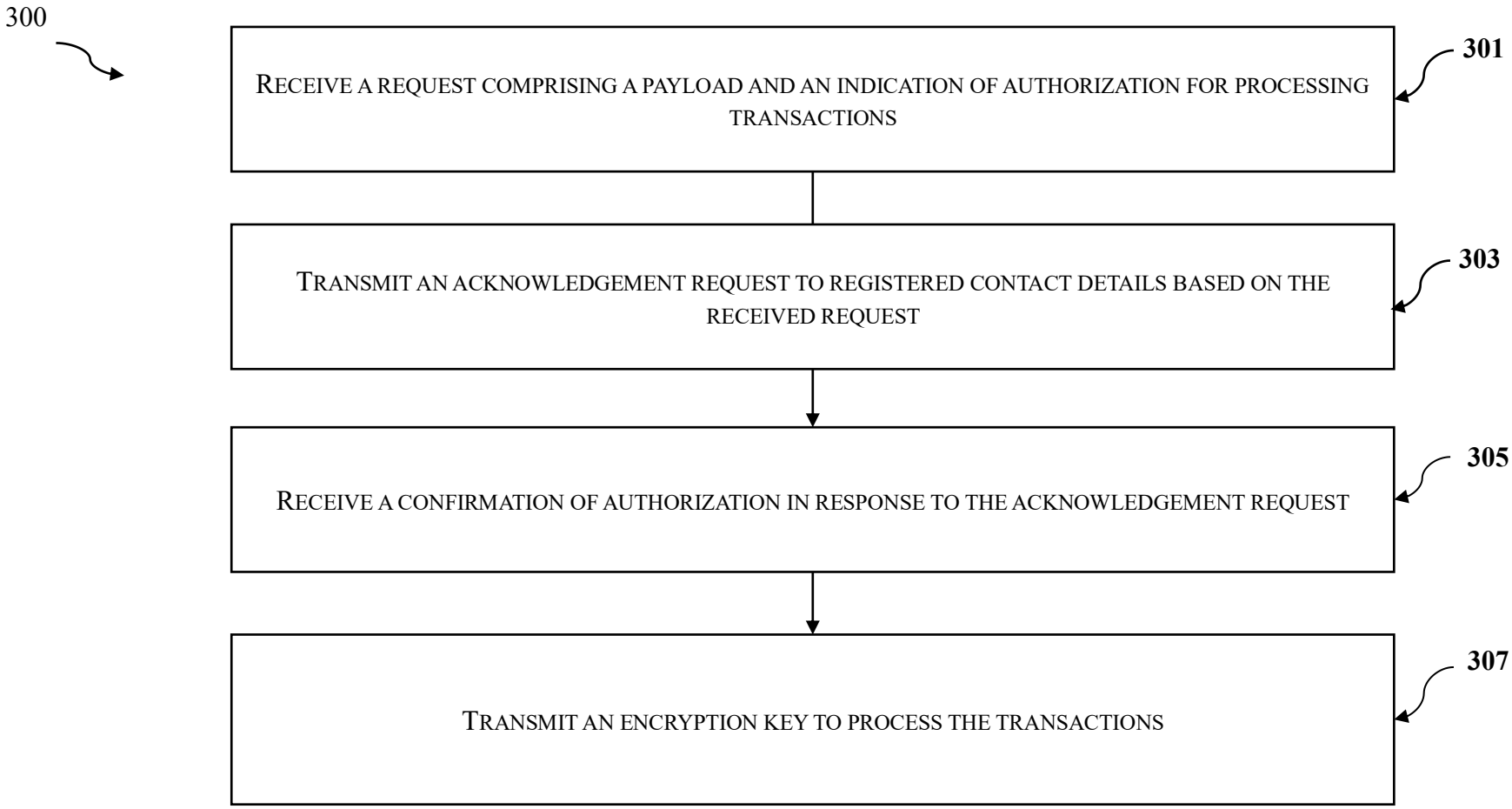
300
RECEIVE A REQUEST COMPRISING A PAYLOAD AND AN INDICATION OF AUTHORIZATION FOR PROCESSING TRANSACTIONS
301
TRANSMIT AN ACKNOWLEDGEMENT REQUEST TO REGISTERED CONTACT DETAILS BASED ON THE RECEIVED REQUEST
303
RECEIVE A CONFIRMATION OF AUTHORIZATION IN RESPONSE TO THE ACKNOWLEDGEMENT REQUEST
305
TRANSMIT AN ENCRYPTION KEY TO PROCESS THE TRANSACTIONS
307

**Fig. 3**