October 2023

OBO (ON BEHALF OF) MULTI FACTOR AUTHENTICATION

BHANU PRATAP SETH Visa

SANGEETA PATNAIK Visa

BIPUL BUSHAN JHA Visa

KANIKA DUREJA Visa

SURESH KALAKRISHNAN Visa

TITLE: “OBO (ON BEHALF OF) MULTI FACTOR AUTHENTICATION”

VISA

BHANU PRATAP SETH

BIPUL BUSHAN JHA

SANGEETA PATNAIK

KANIKA DUREJA

SURESH KALAKRISHNAN

TECHNICAL FIELD

[0001] This disclosure generally relates to the field of transaction authentication techniques. More particularly, the present disclosure focuses on payment card security and multi-factor authentication on behalf of cardholders.

BACKGROUND

[0002] A payment card, such as a credit card or a debit card, enables a cardholder to perform various tasks, such as cash withdrawal or cashless transactions at a physical point of sale (POS) and online transactions through a device for various activities. For a cashless transaction to be performed, the cardholder may swipe or tap the card at the POS or enter the card details on an online platform. These details may include the cardholder's name, card identification number, expiry details, or CVV. However, any person other than the authorized cardholder may access these details and use them to complete a transaction. To address the unauthorized access to the details, a multi-factor authentication method has been introduced by the card issuing companies. The multi-factor authentication method enhances security of the transaction by asking one-time password (OTP) from a cardholder. When the card is swiped at the POS or the card details are entered on the online platform, an OTP is required to complete the transaction. The OTP may be sent to the cardholder via SMS which is sent to a registered phone number or the OTP may be sent to the registered email of the authorized user. This ensures that a person conducting the transaction is an authorized person.

[0003] However, there are many instances where the cardholder may not be able to authenticate the transaction by himself/herself or it may not be safe for the cardholder to authorize the transaction. For example, the device/phone may read out loud the OTP or PIN using an inbuilt text-to-speech tool designed to serve accessibility requirements for visually impaired people while authenticating the transaction, which he/she might not find comfortable and safe in public space. Further, while travelling to abroad, a person’s registered sim card may not active to receive the OTP. Also, sometimes parents give their cards to their kids, but they may want to authenticate every purchase by themselves. So there is a need to design a system that can address all the above problems.

SUMMARY

[0004] According to some non-limiting embodiments, the present disclosure discloses system and method for authenticating a transaction on behalf of cardholders who may not be able to authorize the transaction. The system allows a cardholder to designate an authorized user for multi-factor authentication (OTP via SMS). Particularly, the cardholder may designate the authorized user to authorize the transaction on their behalf. There may be various scenarios where the cardholder may encounter challenges in authenticating the transaction or where safety concerns arise, and they require a designated person who can authorize the transaction on their behalf. The present disclosure provides an efficient and secure way where the designated authorized user may authorize the transaction on behalf of the cardholder. The authorized user may be one or more of the following, but not limited to, a family member, friend or attorney who may authenticate the transaction on behalf of the cardholder.

[0005] The foregoing summary is illustrative only and is not intended to be in any way limiting. In addition to the illustrative aspects, embodiments, and features described above, further aspects, embodiments, and features will become apparent by reference to the drawings and the following detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS AND APPENDICES

[0001] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and together with the description, serve to 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 and/or methods in accordance with embodiments of the present subject matter are now described below, by way of example only, and with reference to the accompanying figures.

[0006] FIG. 1 illustrates an exemplary representation of account creation on the authenticator app and designating an authorized user, in accordance to an embodiment of the present disclosure;

[0007] FIG. 2 discloses an exemplary workflow of transaction authentication by an authorized user when an authenticator application is installed on the authorized user’s device, in accordance to an embodiment of the present disclosure; and

[0008] FIG.3 shows a workflow that illustrates transaction authentication by an authorized user when the authenticator application is not installed on the authorized user's device, in accordance to an embodiment of the present disclosure.

[0009] It should be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative systems embodying the principles of the present subject matter. Similarly, it will be appreciated that any flowcharts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and executed by a computer or processor, whether or not such computer or processor is explicitly shown.

DESCRIPTION OF THE DISCLOSURE

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

[0014] As used herein, the term “merchant” may refer to a company or individual that receives payments from customers for the products or services they provide. The merchant may be, but not limited to an e-commerce website, a retail store, or any other entity offering goods or services for purchase. As used herein, the term “acquirer” may refer to a bank, financial institution, and so forth. The acquirer authorizes the transaction by verifying funds with the issuing bank and settles the funds by transferring money. The acquirer may have a database in which the information related to transaction details, account balance, etc. is stored. As used herein, the term “issuer” may refer to the bank that issues the cards to the consumer. In the transaction process, the issuer may manage the authorization of a transaction. The issuer may authenticate that the card being used belongs to the cardholder and have sufficient funds or credit for it. As used herein, the term “Payment networks” may refer to “networks” that facilitate the authorization, routing, and settlement of transactions a payment process. The payment networks act as intermediaries between merchants, issuers, and acquirers. They ensure that the transactions are securely processed and that funds are transferred from the customer's account to the merchant's account.

[0015] It will be apparent that systems and/or methods, described herein, can be implemented in different forms of hardware, software, or a combination of hardware and software. The actual specialized control hardware or software code used to implement these systems and/or methods is not limiting the implementations. Thus, the operation and behavior of the systems and/or methods are described herein without reference to specific software code, it is understood that software and/or hardware can be designed to implement the systems and/or methods based on the description herein.

[0016] A skilled person would appreciate that authentication is essential for ensuring the security and integrity of financial transactions. It is very critical to verify the transaction by authenticating it to maintain trust and confidence in the global financial system. Thus, the present disclosure provides enhanced authentication capability for issuers under a secure network and enables cardholders to perform uninterrupted operations using a trusted source.

[0017] The present disclosure discloses the concept of an authenticator application to allow an authorized user to authenticate a transaction on behalf of (OBO) of a cardholder. The authenticator application may be installed on a device or may be used in a browser. The authenticator application may have the details of the cardholder and authorized user stored therein. The need to authorize a person to authenticate the transaction on behalf of the cardholder may arise in various situations as described in the earlier paragraphs, but not limited thereto. For example, when the cardholder is visually impaired or when the cardholder is travelling abroad and may not be able to receive/share the authentication code (OTP), or sometimes parents may want to authenticate every purchase done by their kids by themselves. Hence, OBO (on behalf of) techniques provide security and better control on authentication of transactions.

[0018] Fig 1 illustrates a method to designate or authorize a user to authenticate transactions on behalf of a cardholder. At step 1, a cardholder (102) may create his account in an issuer application and may provide details such as PAN, email ID, contact numbers of a person/user (106) to whom the cardholder (102) may want to authorize to perform transactions on behalf of him/her. The issuer application (108) may store the details of the person such as PAN, email ID and phone numbers. The application may also store information related to the cardholder (102). Further, at step 2, the issuer application (108) may send the details of the authorized person (106) and the cardholder (102) to the issuer (104). Further, at step 3, the issuer (104) may send a notification to the authorized person's (106) device, which may have instructions to install and download an authenticator application (110). Upon receiving the notification from the issuer (104), the authorized person (106) may download and install the authenticator application (110), at step 4. The authorized person (106) may create an account by providing his/her details and may set up his/her preferred authentication method, such as biometrics or OTP, but not limited thereto. At step 5, the authenticator application (110) may communicate with the issuer (104) to validate the mapping between the cardholder (102) and the authorized person's (106) details. Moving to step 6, upon verification of the details of the authorized person (106) by the issuer bank (104), an account may be successfully created for the authorized person in the authenticator application (110). At step 7, after completion of the steps 1 to 6, the authorized person (106) may receive a confirmation notification. At step 8, the issuer may send a confirmation notification to the issuer application (108). Finally, at step 9, the cardholder (102) may receive a confirmation notification from the issuer application (108),

marking the completion of the process. In this manner, a person may be designated or authorized to authenticate transactions on behalf of the cardholder. The cardholder may choose an option to designate the authorized user for the multi-factor authentication from multiple options a) send to both, which include card holder as well as the authorized user b) send to only the authorized user and c) send to only the cardholder.

[0019] Figure 2 illustrates a method of authenticating a transaction by an authorized user on behalf of a cardholder when an authenticator application (110) is installed on the authorized user's (106) device, in accordance with an embodiment of the present disclosure. The method may be implemented in a scenario where the cardholder (102) initiates a transaction, but he is not able to authenticate the transaction by himself. This situation may arise in various scenarios such as when the registered phone number is inactive (for example, during travel to a different country with no active cellular network to receive an OTP to authenticate the transaction), or when the cardholder is visually impaired and faces difficulty to complete the transaction, but not limited thereto. In such cases where the cardholder may not be able to authenticate the transaction, the authorized user may authenticate the transaction on behalf of the cardholder. The transaction may be authorized via the authenticator app (110) installed on the authorized user's device.

[0020] In an embodiment, the cardholder (102) may initiate a transaction by swiping the card through a Point of Sale (PoS) terminal or by entering the card details by the user into a merchant's (212) platform as such e-commerce website, but not limited thereto. The merchant (212) may forward transaction details including the card details to the acquirer (214) to authorize the transaction. The acquirer may forward the received details to a payment network (216) for further processing. In response, the card network (216) may request authorization from the issuer (104).

[0021] Upon receiving the request, the issuer (104) may check the authentication type. For instance, the issuer (104) may check whether the authentication type is "OBO". When the authentication type is "OBO", the issuer (104) may retrieve the authorized user's (106) details. Subsequently, after retrieving the details of the authorized user (106), the issuer (104) may transmit a transaction authentication request through a push notification to the authorized user's (106) device. In response, the authorized user (106) may log into the authenticator application (110) to review the transaction details to verify the transaction details. Once the authorized user (106) approves/authenticates the transaction, the issuer (104) may receive confirmation of the

successful transaction. This confirmation of approval is subsequently communicated to both the cardholder (102) and the merchant (212), thus allowing the transaction to be completed securely.

[0022] In another embodiment, it may be possible that the authenticator application (110) may not be installed on the authorized user's (106) device. Figure 3 illustrates a method of authenticating a transaction by an authorized user on behalf of a cardholder when an authenticator application (110) is not installed on the authorized user's (106) device, in accordance with an embodiment of the present disclosure. In this case when the payment network (216) requests the issuer (104) for authorization, the issuer (104) first checks whether the authentication type is OBO or not. When the authentication type is OBO, the issuer (104) may fetch the details of the authorized user (106) and may send an authentication request to the authorized user (106). The authentication request may comprise a link or URL of a webpage to authenticate the transaction. The authorized user (106) may access the link or the URL and may perform initial set up by providing required details. Upon setup, the details of the authorized user (106) may be verified by the issuer by mapping the details of the authorized user with details given by the cardholder in the issuer application. Upon verification of the details, the transaction details may be presented before the authorized user (106) for his approval. When the authorized user (106) approves the transaction, the issuer (104) may receives confirmation of the successful transaction. Further, the confirmation may also be sent to the cardholder (102) and transaction may be completed.

[0023] In this manner, the disclosed method and system provide an uninterrupted and hassle-free payment authentication experience for the cardholders. The on behalf of (OBO) authentication technique helps the cardholder to designate an authorized user who can authorize the transaction on their behalf. Numerous scenarios exist where the cardholder encounters challenges in authenticating the transaction or where safety concerns arise, and they require a designated person who can authorize the transaction on their behalf. The present invention provides an efficient and secure way where the designated authorized user may authorize the transaction on behalf of the cardholder.

[0024] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure.

[0025] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0026] 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.).

[0027] 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.

[0028] 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.

[0029] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to being prior art.

[0030] Although the invention has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred embodiments, it is to be understood that such detail is solely for that purpose and that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the invention. For example, it is to be understood that the present invention contemplates that, to the extent possible, one or more features of any embodiment can be combined with one or more features of any other embodiment.

“OBO (ON BEHALF OF) MULTI FACTOR AUTHENTICATION”

ABSTRACT

The present disclosure relates to an authentication method to enable a person to authenticate transaction on behalf of the cardholder. On behalf of (OBO) authentication allows the card holder to designate an authorized user to authenticate on behalf of them for multi factor authentication, login or any other operation. When the cardholder initiates the transaction, a request to authorize the transaction may be sent to the authorized user, and the authorize user may approve the transaction on behalf of the cardholder.

Fig. 1

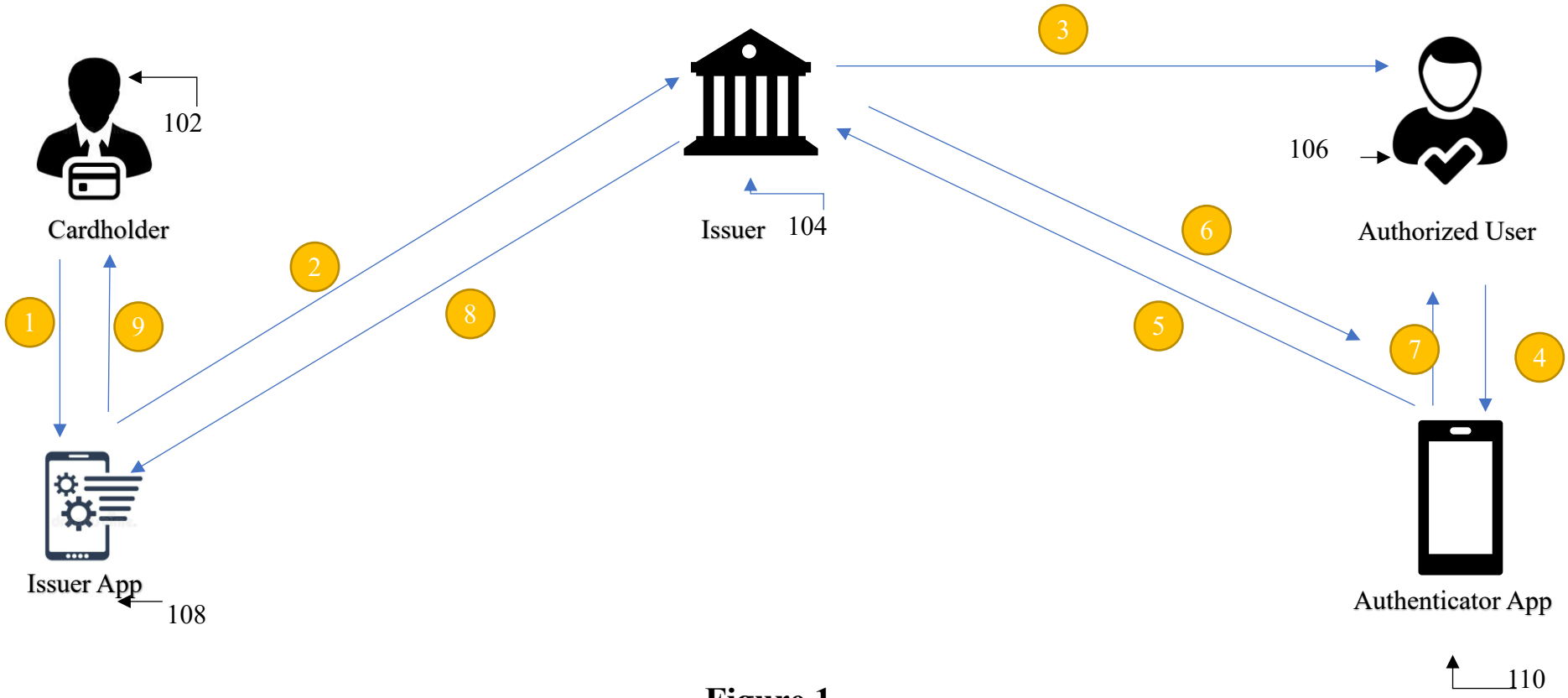
102
Cardholder
Issuer
104
106
Authorized User
Issuer App
108
Authenticator App
110
1
2
3
4
5
6
7
8
9

Figure 1

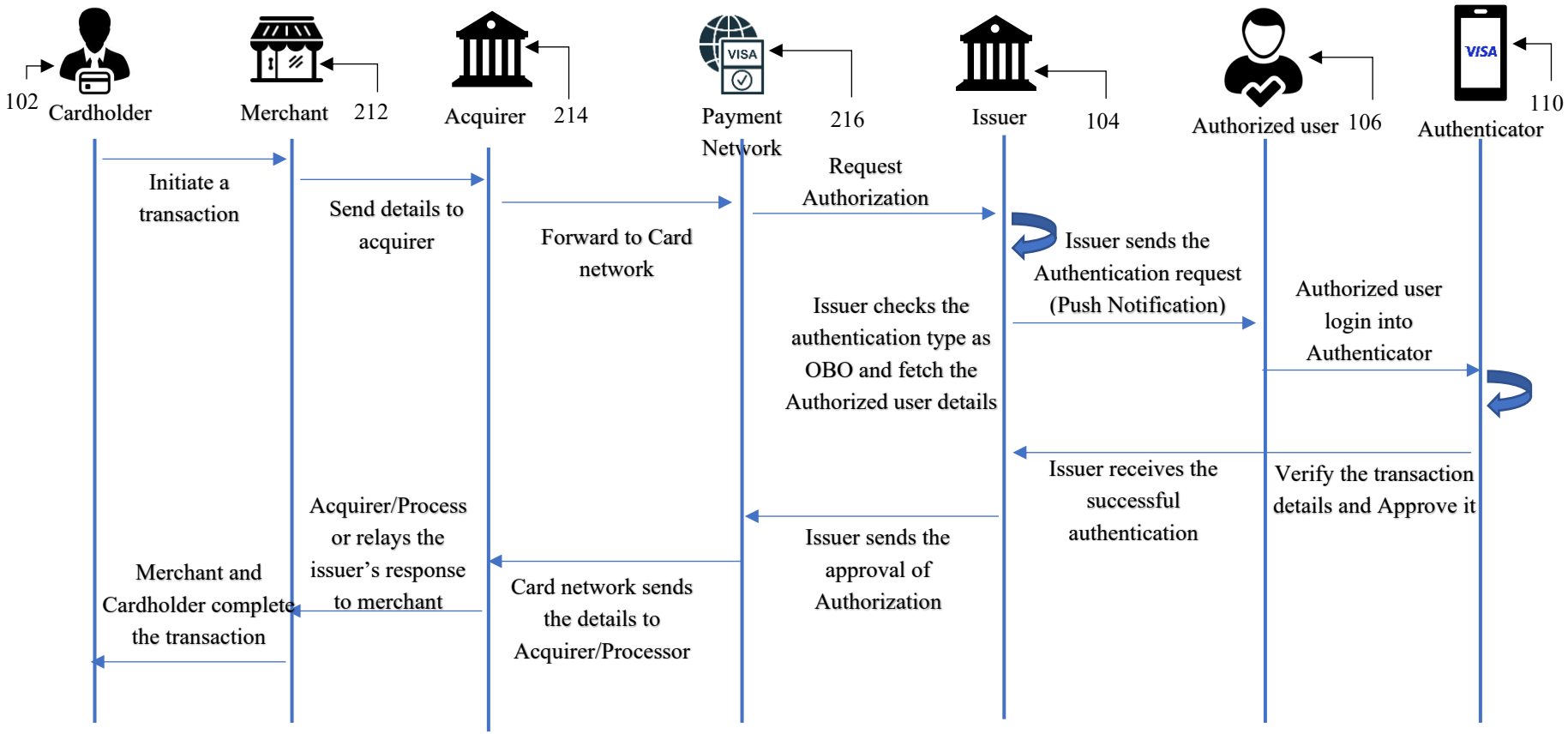
102
Cardholder
Merchant
212
Acquirer
214
Payment Network
216
Issuer
104
Authorized user
106
Authenticator
110
Initiate a transaction
Send details to acquirer
Forward to Card network
Request Authorization
Issuer sends the Authentication request (Push Notification)
Authorized user login into Authenticator
Issuer checks the authentication type as OBO and fetch the Authorized user details
Issuer receives the successful authentication
Verify the transaction details and Approve it
Issuer sends the approval of Authorization
Card network sends the details to Acquirer/Processor
Acquirer/Process or relays the issuer's response to merchant
Merchant and Cardholder complete the transaction

Figure 2

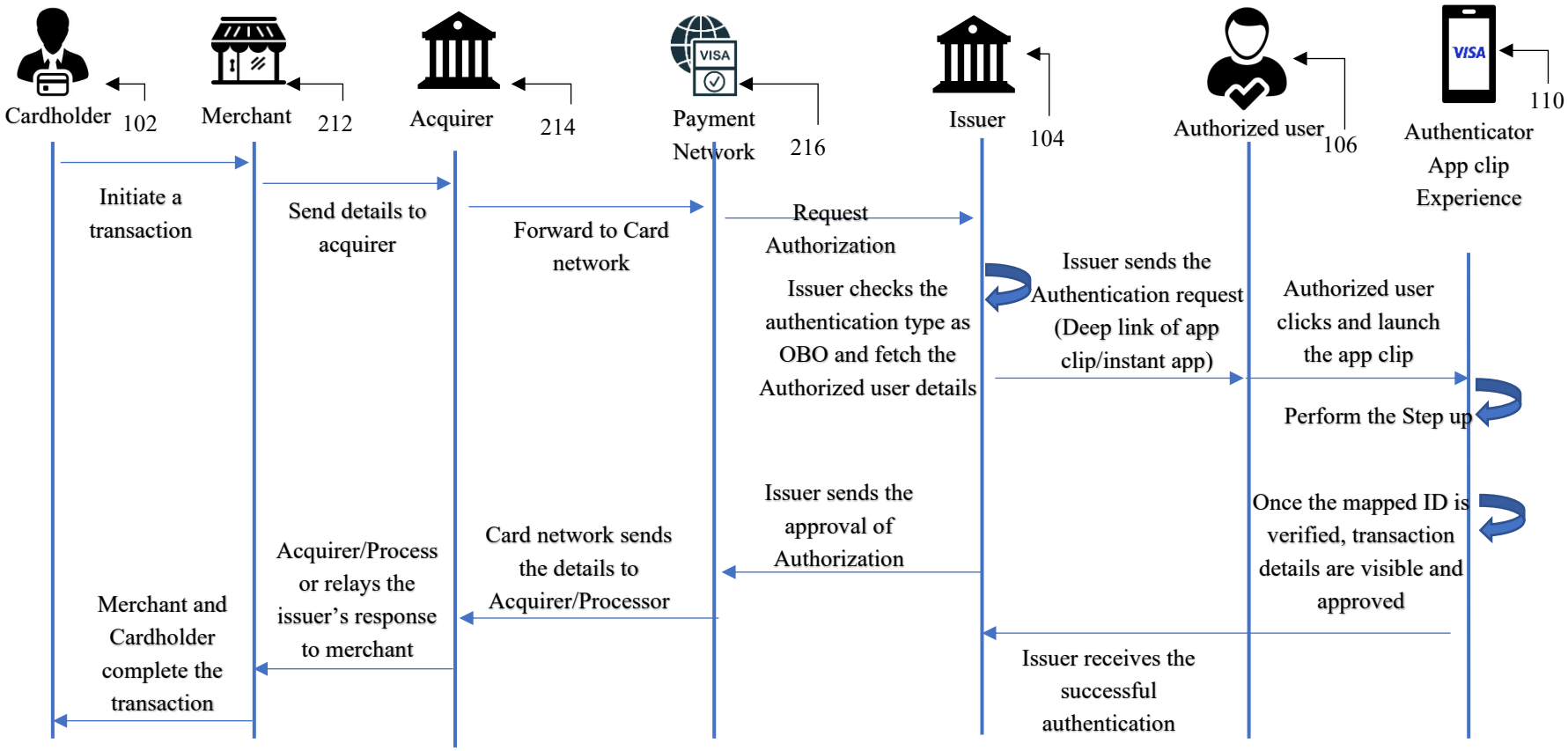
Cardholder
102
Merchant
212
Acquirer
214
Payment Network
216
Issuer
104
Authorized user
106
Authenticator App clip Experience
110
Initiate a transaction
Send details to acquirer
Forward to Card network
Request Authorization
Issuer checks the authentication type as OBO and fetch the Authorized user details
Issuer sends the Authentication request (Deep link of app clip/instant app)
Authorized user clicks and launch the app clip
Perform the Step up
Once the mapped ID is verified, transaction details are visible and approved
Issuer receives the successful authentication
Issuer sends the approval of Authorization
Card network sends the details to Acquirer/Processor
Acquirer/Process or relays the issuer's response to merchant
Merchant and Cardholder complete the transaction

Figure 3