

Technical Disclosure Commons

Defensive Publications Series

June 2023

NEAR FIELD COMMUNICATION (NFC) AND SECURE ELEMENT (SE) INTEGRATED GAMING CONTROLLER

Yuexi Chen

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Chen, Yuexi, "NEAR FIELD COMMUNICATION (NFC) AND SECURE ELEMENT (SE) INTEGRATED GAMING CONTROLLER", Technical Disclosure Commons, (June 26, 2023)

https://www.tdcommons.org/dpubs_series/5999



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

**“NEAR FIELD COMMUNICATION (NFC) AND SECURE
ELEMENT (SE) INTEGRATED GAMING CONTROLLER”**

VISA

INVENTOR: Yuexi Chen

TECHNICAL FIELD

[0001] The present subject matter is, in general, related to the field of gaming consoles. In particular, the subject matter relates to facilitating frictionless payment experience and convenient switching between the gaming consoles.

BACKGROUND

[0002] The following description includes information that may be useful in understanding the present invention. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

[0003] The gaming industry has seen an exponential rise in the past few years. As it captures a substantially large market share, more and more digital assets are being sold on video gaming consoles, including subscriptions, downloadable content, online courses, templates, etc.

[0004] Now the payment of these digital assets are generally managed by remote e-commerce transactions like card on file, e-com token etc. However, these payment methods do not offer a smooth interface for a user to make the payments and involve a trail of cumbersome processes. Further, the process becomes more incommodious when the gaming consoles operate without a keyboard, a mouse, or a browser.

[0005] Also, since the user's payment credentials and authorizations are usually associated with a particular gaming console or account, the user faces operational difficulties when switching between the gaming consoles.

[0006] Hence there is a need for a method and a system thereof that overcomes the limitations of the existing mechanisms and facilitates an easy payment process while also ensuring smooth transition for the user who wants to move between different consoles.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] 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 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:

[0008] Fig. 1A illustrates a gaming controller in front view with NFC (Near Field Communication) antenna and SE, in accordance with an embodiment of the present disclosure.

[0009] Fig. 1B illustrates a user tapping the contactless card for payment of digital assets on the NFC antenna of the gaming controller, in accordance with an embodiment of the present disclosure.

[0010] Fig. 2 illustrates a block diagram of a system for facilitating frictionless payments and user authentication process, in accordance with an embodiment of the present disclosure.

[0011] Fig. 3 illustrates a flow diagram illustrating an exemplary embodiment involving a method of making the payment through a contactless card tap, in accordance with an embodiment of the present disclosure.

[0012] Fig. 4 illustrates a flow diagram illustrating a method of provisioning a device token to bind the user account with the generated device token, in accordance with an embodiment of the present disclosure.

[0013] Fig. 5 illustrates a flow diagram illustrating a method of making the payment through the device token associated with the gaming controller without involving the need for contactless card tap, in accordance with an embodiment of the present disclosure.

[0014] Fig. 6 illustrates a flow diagram illustrating a method for enabling, for a user, frictionless transition between different gaming consoles, in accordance with an embodiment of the present disclosure.

[0015] 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

[0016] 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.

[0017] 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.

[0018] 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.

[0019] The terms “comprise”, “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 preceded by “comprises... a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

[0020] 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.

[0021] The terms “including”, “comprising”, “having” and variations thereof mean “including but not limited to” unless expressly specified otherwise.

[0022] The gaming industry has become a lucrative arena for advertising and selling of products and various digital assets along with subscriptions and memberships. But since the payment of these digital assets is generally managed by remote e-commerce transactions like card on file and e-com token, they do not offer a smooth interface for a user to make the payments and the process becomes more incommodious when the gaming consoles operate without a keyboard, a mouse, or a browser. Furthermore, users find the process of moving between the different gaming consoles fraught with friction as the digital assets of the user are associated with the registered account on the gaming platform and in order to switch between gaming consoles, user has to again login to the registered account and validate the gaming controller associated with that account every time he/she wishes to transition to a new gaming console. Further, switching between different gaming consoles may also result in compromising the security of transactions performed by a user on a new gaming console.

[0023] To overcome these challenges, the present disclosure provides for a gaming controller which is equipped with an NFC antenna and a Secure Element (SE) that detects the contactless card tap for payment for digital assets in a game or on the gaming platform and then provides a device token which gets bound with the concerned gaming controller. The device token can be seamlessly used to make payments and move the gaming controller between different consoles thus providing a better user experience. A detailed explanation of the proposed solution is disclosed in the forthcoming paragraphs.

[0024] **Fig 1A** illustrates a front view of a gaming controller 102 which includes a controller body, a holding area 104 for the gaming controller 102 and push buttons/key/arrows 108 to provide inputs while playing a game, in accordance with an embodiment of the present disclosure. However, it may be noted by a skilled person that the gaming

controller 102 is not restricted to the one depicted in Fig 1A and may also include game pads, joysticks, joypads, fight sticks etc. Further, the gaming controller 102 is equipped with an NFC antenna 106 which is capable of detecting an NFC enabled payment card in order to provide payments for the concerned digital assets. This has been further explained in detail in the forthcoming paragraphs in conjunction with Fig 1B and Fig 2 of the present disclosure.

[0025] Fig 1B illustrates a user 112 holding an NFC enabled contactless payment card 110 near the NFC antenna 106 of the gaming controller 102, as shown in figure 1A. The contactless payment card 110 tap activates a reader of the NFC antenna 106 to read the information on the contactless payment card 110. It may be noted by a skilled person that the contactless payment card 110 may comprise different types of NFC enabled payment cards like debit card, credit card or any other payment device. This has been further explained in forthcoming paragraphs in conjunction with Fig 2 of the present disclosure.

[0026] Fig 2 depicts an exemplary block diagram 200 illustrating a system 202 for facilitating frictionless payments and user authentication process in accordance with the embodiment of the present disclosure. The system 202 comprises a gaming controller 210 and a server 230 in communication with each other. The gaming controller 210 comprises an NFC antenna 212, an NFC frontend 214, an I/O Interface 216, a Secure Element (SE) 218, a processing unit 220, and a memory 222. The processing unit 220 may be operatively coupled to the NFC frontend 214, the I/O Interface 216, the SE 218 and the memory 222. The gaming controller 210 communicates with the server 230 which in turn comprises a memory 232, a transceiver 234 and a processing unit 236. Further, in one implementation, the processing units 220 and 236 may be implemented as one or more microprocessors, microcomputers, microcontrollers, digital signal processors, central processing units, state machines, logic circuitries, and/or any devices that manipulate signals based on operational instructions. The I/O interface 216 may include a variety of software and hardware interfaces, for example, a web interface, a graphical user interface, and the like. Further, among other capabilities, the processing unit 236 may be configured to fetch and execute computer-readable instructions stored in the memory 232 of the server 230.

[0027] Now referring back to Fig 1B, when the user 112 wants to make payment for any digital asset being displayed on the gaming console, in one non-limiting embodiment, the user 112 may bring the contactless payment card 110 near the NFC antenna 106 of the gaming controller 102 such that the contactless payment card 110 may fall in the vicinity of the near field region of the NFC antenna 106. In another non-limiting embodiment, the user 112 may also tap the contactless payment card 110 on the NFC antenna 106 to initiate the process of payment. When the contactless payment card 110 is tapped on the NFC antenna 106, the NFC frontend 214, which is a type of NFC reader, is activated to read the information on the contactless payment card 110. The NFC frontend 214 may thus facilitate the connectivity between the gaming controller 102 and the contactless payment card 110. Further, in one aspect, the contactless communication (facilitated by Application Protocol Data Unit (APDU) exchange) between the gaming controller 210 and contactless payment card 110 may be wrapped into wireless protocol and wired protocol between the gaming console and the gaming controller 210. In one of the non-limiting embodiments, the wireless protocol may be enabled through Bluetooth and the wired protocol may be facilitated through USB. Further, the NFC frontend 214 may read the sensitive information on the contactless payment card 110 through APDU exchange and may obtain a cryptogram associated with it, which may be further used for online authentication of the respective contactless payment card 110. This captured cryptogram may then be sent to the issuer of the contactless payment card 110 for approval, thus enabling the issuer to authenticate the payment request and further add a layer of security to the payment process.

[0028] In yet another non-limiting embodiment, the system 202 may facilitate generation of a device token associated with the gaming controller 210 to avoid the need for tapping the contactless payment card 110 every time the user wishes to make a purchase for a digital asset. To facilitate this, once the contactless payment card 110 is read by the NFC frontend 214 and APDU exchange has obtained the cryptogram associated with it, a pop up may be displayed on the gaming console that reads “remember this card on my controller” in one non-limiting embodiment. If the user 112 selects “remember this card on my controller”, then the contactless payment card 110 details may be saved in the memory 222 of the associated gaming controller 210. Subsequently, an identification and verification (ID&V) process may be initiated to authenticate the user 112 by the issuer of the contactless payment card 110. This ID&V process may be

accomplished by one or more means including, but not limited to, CVV code, SMS or OTP associated with the registered mobile number of the user 112.

[0029] Once the issuer of the contactless payment card 110 authenticates the user 112, then the Secure Element (SE) 218 of the gaming controller 210 may send the stored SE data like serial number, certificate, public key, etc. associated with the gaming controller 210 to the server 230. It may be noted by a skilled person that the SE data may be unique for each gaming controller 210 and may thus help in authorizing unique ID for each one of them. Moving on, the server 230 may receive the SE data through a transceiver 234 and may generate an encrypted device token via its processing unit 236. The device token may include any unique reference ID and may not necessarily be limited to tokens, secret symmetric and asymmetric keys, payment account reference (PAR) etc. This encrypted device token generated at the server 230 may then be sent back to the gaming controller 210 by transceiver 234 of the server 230. In another embodiment, to add another layer of security, the user 112 may also be required by the system 202 to verify the identity of the user 112 and in turn that of the gaming controller 210. This may be done by means of a personal identification code like a security PIN etc. associated earlier with the specific registered account by using buttons 108 combination of the gaming controller 210. This security authentication is not necessarily limited to personal ID code and can also include biometric verifications etc. if supported by the gaming controller 210. After authentication by the user 112, the gaming controller 210 may bind that specific device token/PAR with that particular gaming controller 210 and the same may be stored in the memory 232 of the server 230.

[0030] Once a unique device token/PAR is associated with the gaming controller 210, the user 112 may make payments for the purchase of digital assets without any requirement of the contactless payment card 110. So, when the purchase is to be made by the user 112 in a game or on the gaming platform store, a unique device token may be detected by the system 202 provisioned on the gaming controller's 210 secure element (SE) 218. The user 112 may then be prompted to press button(s) 108 as personal identification code, or a biometric authentication may be done on the gaming controller 210 as cardholder verification method. APDU command/response may be exchanged and authorization request with captured cryptogram may then be sent to issuer of the contactless payment card 110 for approval.

[0031] In another embodiment, the user 112 may wish for one or more additional users such as friends, family etc., to be able to make transactions for the purchase of digital assets through the contactless payment card 110 whose details are already stored in the gaming controller 210. In such a scenario, the user 112 may provide the details of the one or more additional users and the authentication of each of the one or more additional users may be accomplished by means of corresponding personal identification codes. In one aspect, each of the additional users shall be required to use buttons 108 of the gaming controller 210 to generate a unique personal identification code. However, it may be noted by a skilled person that such authentication may not be required when the one or more additional users use the contactless payment card 110 each time for making the transaction. Hence, the authentication procedure may only be facilitated when the contactless payment card 110 is bound to the gaming controller 210 and the one or more additional users may wish to use the saved card to make payments.

[0032] Therefore, by means of the disclosure provided in the above paragraphs, the system 202 may facilitate frictionless payment of various digital assets in a game or on the gaming platform by the user 112. Next, the system 202 may also facilitate seamless switching between the gaming consoles by the user 112. The same has been described in the forthcoming paragraphs.

[0033] In one exemplary scenario, the user 112 playing a game on the gaming controller 210 connected to a particular gaming console may want to switch to another console to play with friends or may want to add another gaming controller to his/her own gaming console. To facilitate this, once the device token/PAR associated gaming controller 210 is connected to a new gaming console, the device token provisioned on its SE 218 may be detected by the new gaming console platform. Subsequently, the new gaming console may facilitate gaming controller's 210 authentication by means of at least one personal identification code, biometric identification etc. Upon authentication, the device token/PAR may be pulled by the new gaming console and the gaming platform may mapped back to the user's 112 original account. This may allow the user 112 to permanently move to a new gaming console.

[0034] However, if the user 112 wants to play on a new gaming console only for a while, then the user 112 may migrate the digital assets associated with the original gaming console to the new gaming console by logging in as a guest player. Once the gaming controller 210 is disconnected from the new gaming console, then the digital assets associated with it may also be erased on the new gaming console. This facilitates players to switch easily between the gaming consoles along with the digital assets associated with their game or the gaming platform seamlessly.

[0035] The disclosed system 200 therefore provides easy payment process of digital assets in a game or on the gaming platform by using a contactless payment card 110 tap or by associating a device token with the gaming controller 210 and it also helps the user 112 to move conveniently between the different gaming consoles without any friction. Furthermore, the system 200 ensures that the account information of the user 112 is secure and is not compromised even when moving between different gaming consoles.

[0036] **Figure 3** illustrates a flowchart 300 of an exemplary method of making the payment through a contactless card tap. The method 300 may also be described in the general context of computer executable instructions. Generally, computer executable instructions may include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform specific functions or implement specific abstract data types.

[0037] The order in which the method 300 is described is not intended to be construed as a limitation, and any number of the described method blocks may be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described.

[0038] At step 302, the method 300 may include tapping the contactless payment card 110 on the NFC antenna 106, 212 of the gaming controller 102, 210 to make the purchase of any digital asset in the game or on the gaming platform. Further, in one non-limiting embodiment, step 302 may include bringing the contactless payment card 110 in vicinity of the NFC antenna 106, 212 of the gaming controller 102, 210. Furthermore, a person skilled in the art would appreciate that the gaming controller 102, 210 may include any game pads, joy pads, fight sticks, joy sticks etc. and the contactless payment card 110 has to be NFC enabled.

[0039] At step 304, the method 300 may include activating the NFC antenna 106, 212 integrated on the gaming controller 102, 210 and detecting the contactless payment card 110. In one non-limiting embodiment, for detecting the contactless payment card 110, the processing unit 220 may be used in conjunction with NFC frontend 214 to read the information on the contactless payment card 110.

[0040] Further, upon detection of the contactless card 110 by the NFC antenna 106, 212, the system 202 may give an option to the user 112 to save the payment card 110 information in the memory 232 of the gaming controller 102, 210 by selection “remember this card on my controller”. The details of said method are depicted in the flowchart 400 representing another approach of the method 300 and explained in the forthcoming paragraphs.

[0041] Now referring back to Figure 3, at step 306, the method 300 may include completing the APDU exchange between the gaming controller 102, 210 and the contactless payment card 110 for securing information associated with the contactless payment card 110. In one non-limiting embodiment, completing the APDU exchange between the gaming controller 102 and contactless payment card 110 may be wrapped into wireless protocol and wired protocol between gaming console and the gaming controller 102, 210.

[0042] At step 308, the method 300 may include sending the authorization request to the issuer of the contactless payment card 110 for approval before authorizing the payment.

[0043] **Figure 4** illustrates a flowchart 400 of an exemplary method of provisioning a device token to bind the user account with the generated device token. The method 400 may also be described in the general context of computer executable instructions. Generally, computer executable instructions may include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform specific functions or implement specific abstract data types.

[0044] The order in which the method 400 is described is not intended to be construed as a limitation, and any number of the described method blocks may be combined in any

order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described.

[0045] At step 402, the method 400 may include selecting the “remember this card on the controller” option on the gaming console. In one non-limiting embodiment, after detecting the contactless payment card 110 by the NFC antenna 106, 212 at step 304 of figure 3, a pop up may be displayed on the gaming console screen giving an option to the user 112 to save the contactless payment card 110 details on the gaming controller 102, 210.

[0046] At step 404, the method 400 may include facilitating authentication of the contactless payment card 110 by the issuer before authorizing any payment request. In one non-limiting embodiment, when the user 112 clicks on the pop up of “choose to remember this card on my controller” using the buttons 108 of the gaming controller 102, 210 or in any other suitable way, the gaming controller 102, 210 through the I/O Interface 216 may send a request to the issuer of the contactless payment card 110 to authenticate the user 112.

[0047] At step 406, the method 400 may include sending the game controller’s 102, 210 SE data to the server 230. In one non-limiting embodiment, when the gaming controller 102, 210 receives the authentication from the issuer of the contactless payment card 110, then the gaming controller 102, 210 may send the SE data to the server 230 by one or more communication means.

[0048] At step 408, the method 400 may include generating and encrypting the device token data which may include PAR, symmetric keys etc. and sending it to the gaming controller’s 102, 210 SE 218. In one non-limiting embodiment, for generating and encrypting the device token, processing unit 236 coupled with memory 232 may be used and the encrypted device token may be sent to the SE 218.

[0049] At step 410, the method 400 may include binding a button combination on the gaming controller 102, 210 using the buttons 108 as personal identification code or using a biometric authentication if supported by the gaming controller 102, 210. In one non-limiting embodiment, for binding the buttons 108 for identification and authorization, processing unit 220 may be used in conjunction with the I/O Interface.

[0050] At step 412, the method 400 may include binding the player account with the device token/PAR on the gaming controller 102, 210. In one non-limiting embodiment, after authentication at step 410, for binding the player account with the device token/PAR on the gaming controller 102, processing unit 220 may be used in conjunction with SE 218.

[0051] **Figure 5** illustrates a flowchart 500 of an exemplary method of making the payment through the device token associated with the gaming controller 102, 210 without involving the need for contactless payment card 110 tap. The method 500 may also be described in the general context of computer executable instructions. Generally, computer executable instructions may include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform specific functions or implement specific abstract data types.

[0052] The order in which the method 500 is described is not intended to be construed as a limitation, and any number of the described method blocks may be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described.

[0053] At step 502, the method 500 may include detecting that the connected gaming controller 102, 210 has a token device provisioned on its SE 218 when the user 112 wants to make a purchase of any digital asset while in a game or on the gaming platform. In one non-limiting embodiment, for detecting the device token, the processing unit 220 may be used in conjunction with SE 218.

[0054] At step 504, the method 500 may include choosing the device token instead of the contactless payment card 110 for making the purchase. In one non-limiting embodiment, for choosing the device token, processing unit 220 may be used in conjunction with SE 218.

[0055] However, if the user 112 chooses to use the contactless payment card 110 for making the purchase, method steps 306-308 of Fig 3 may be used.

[0056] Referring back to Fig 5, at step 506, the method 500 may include pressing the buttons 108 on the gaming controller 102, 210 for personal identification code or performing biometric authentication. The buttons pressed at 506 may be compared against the buttons bound to the gaming controller 102, 210 at step 410 of figure 4, for the purpose of authentication. In one non-limiting embodiment, the processing unit 220 may be used in conjunction with SE 218 for authentication of the pressed buttons.

[0057] At step 508, the method 500 may include completing the APDU exchange by kernel with SE 218 on the gaming controller 102, 210 where the kernel may include, but not limited to, on-device kernel, hybrid device/cloud kernel or cloud kernel. In one non-limiting embodiment, for completing the APDU exchange, the processing unit 220 may be used in conjunction with the SE 218 of the gaming controller 220.

[0058] At step 510, the method 500 may include sending the authorization request to the issuer of the contactless payment card 110 for approval before authorizing the payment.

[0059] **Figure 6** illustrates a flowchart 600 of an exemplary method of enabling, for a user 112, frictionless transition between different gaming consoles. . The method 600 may also be described in the general context of computer executable instructions. Generally, computer executable instructions may include routines, programs, objects, components, data structures, procedures, modules, and functions, which perform specific functions or implement specific abstract data types.

[0060] The order in which the method 600 is described is not intended to be construed as a limitation, and any number of the described method blocks may be combined in any order to implement the method. Additionally, individual blocks may be deleted from the methods without departing from the spirit and scope of the subject matter described.

[0061] At step 602, the method 600 may include detecting connection of the user's 112 gaming controller 102, 210 to a new gaming console.

[0062] At step 604, the method 600 may include detecting, at the new gaming console, that the gaming controller 102, 210 has a token device provisioned to its SE 218.

[0063] At step 606, the method 600 may include pressing the buttons 108 on the gaming controller 102, 210 for personal identification code or performing biometric authentication. The buttons pressed at step 606 may be compared against the buttons bound to the gaming controller 102, 210 at step 410 of figure 4, for the purpose of authentication. In one non-limiting embodiment, the processing unit 220 may be used in conjunction with SE 218 for authentication of the pressed buttons.

[0064] At step 608, the method 600 may include pulling the device token by the new gaming console and mapping it back to the user's 112 account associated with it. In one non-limiting embodiment, the device token may be pulled from the memory 232.

[0065] At step 610, the method 600 may include choosing to permanently move to the new gaming console or moving only as guest for some time. If the user 112 wants to play on a new gaming console only for a while, then he/she can migrate the digital assets associated with the original gaming console to the new gaming console by logging as a guest player. After the playing session, once the gaming controller 102, 210 is disconnected, then the digital assets associated with it are also erased on the new gaming console. This facilitates players to move easily between the gaming consoles along with the digital assets associated with their game or the gaming platform seamlessly.

[0066] 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 blocks 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.

[0067] 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.

[0068] Furthermore, 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. The term “computer- readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include random access memory (RAM), read-only memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

[0069] Suitable processors include, by way of example, a general-purpose processor, a special purpose processor, a conventional processor, a digital signal processor (DSP), a graphic processing unit (GPU), a plurality of microprocessors, one or more microprocessors in association with a DSP core, a controller, a microcontroller, Application Specific Integrated Circuits (ASICs), Field Programmable Gate Arrays (FPGAs) circuits, any other type of integrated circuit (IC), and/or a state machine.

**NEAR FIELD COMMUNICATION (NFC) AND SECURE ELEMENT (SE)
INTEGRATED GAMING CONTROLLER**

ABSTRACT

Disclosed herein is a system 202 for providing an NFC 212 and a SE (Secure Element) 218 integrated gaming controller 210. In particular, when a user 112 taps a contactless payment card 110 on the NFC antenna 212 of the gaming controller 210 for purchasing digital assets, a cryptogram of the contactless payment card 110 is obtained through the APDU exchange by the gaming controller 210 and a device token is thereafter provisioned by a server 230 in communication with the gaming controller 210. This associates the user 112 account with the generated device token which is further used to purchase more digital assets in future without the need for tapping the contactless payment card 110. Further, the generated device token also enables the user 112 to conveniently switch between the different gaming consoles to play with teammates without any friction.

[FIG 2]

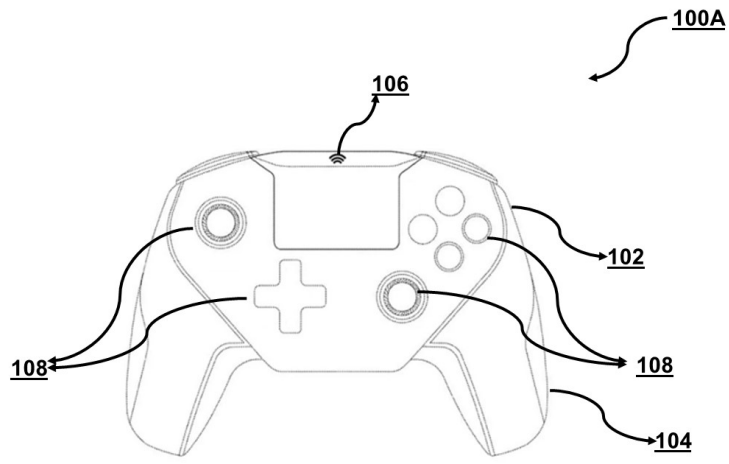


Fig 1A

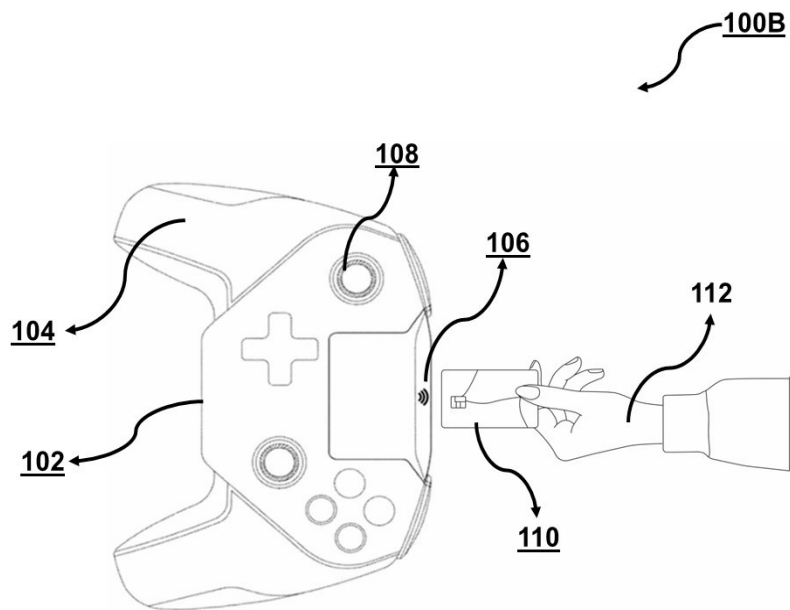


Fig 1B

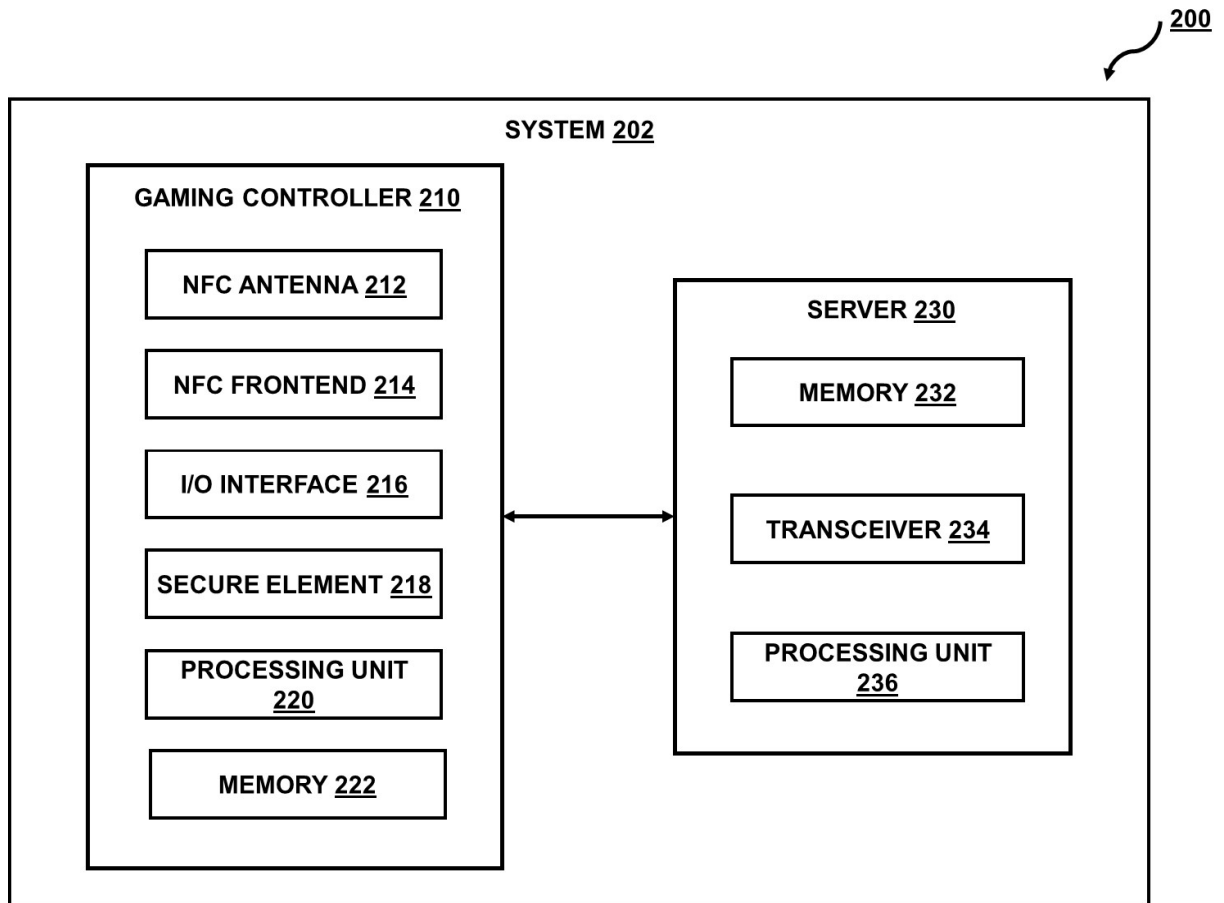


Fig 2

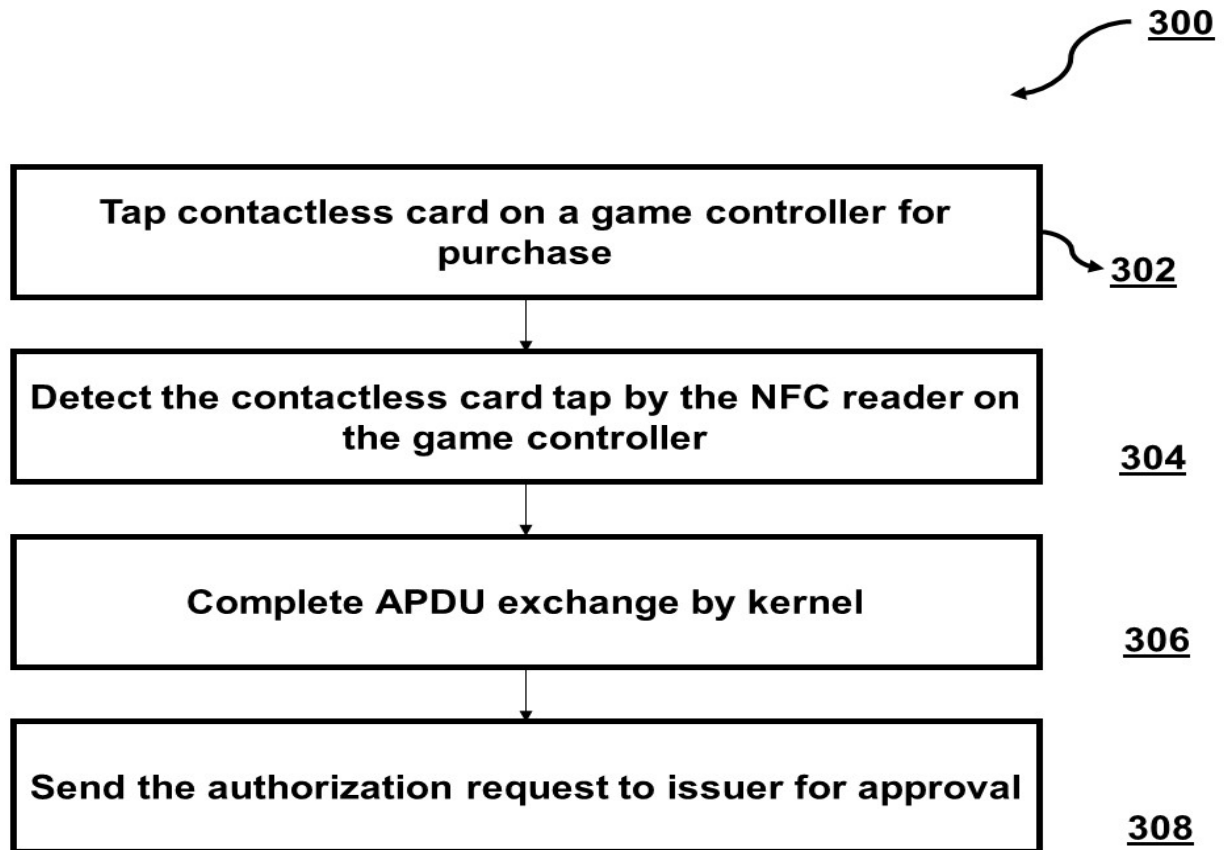


Fig 3

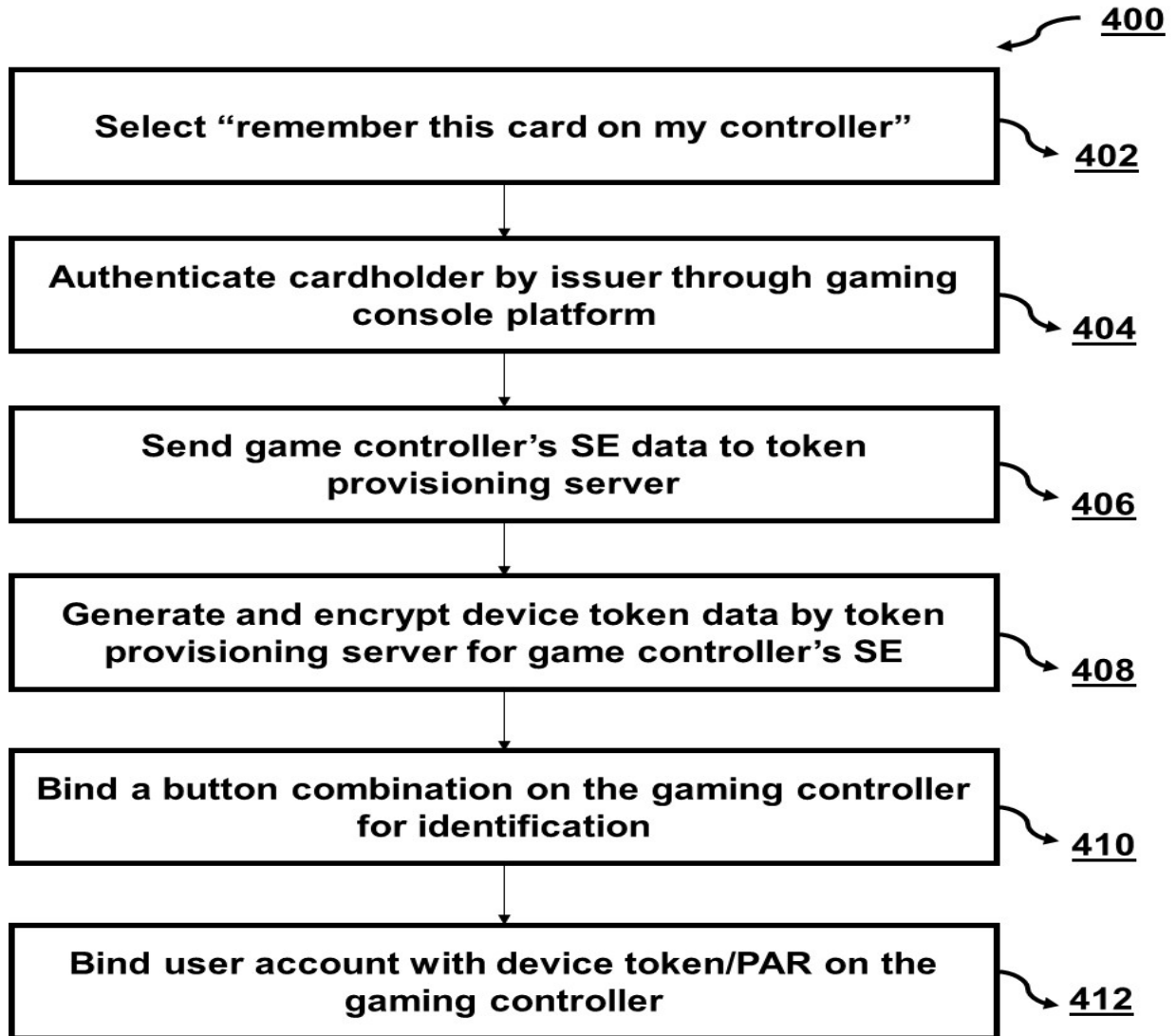


Fig 4

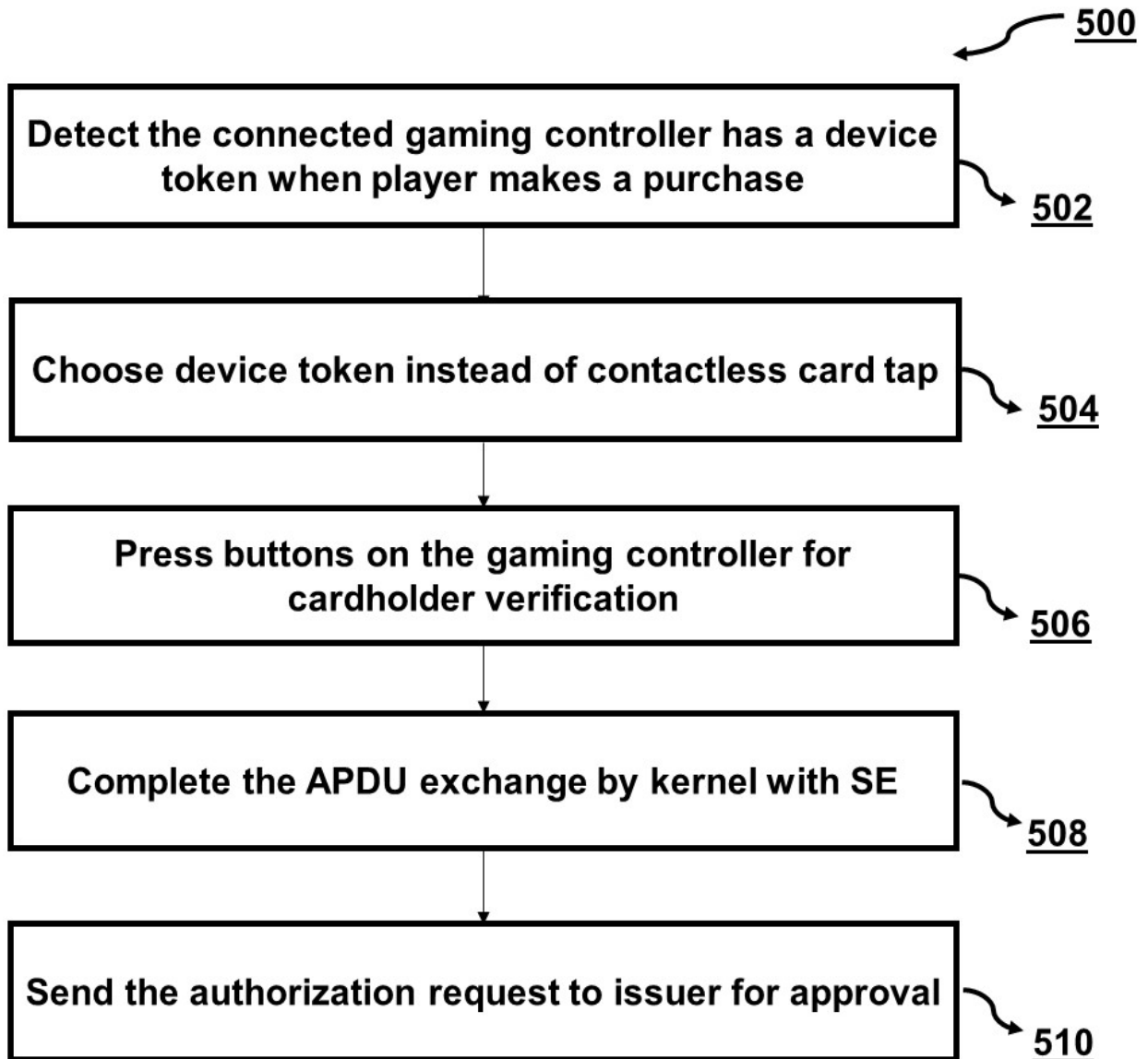


Fig 5

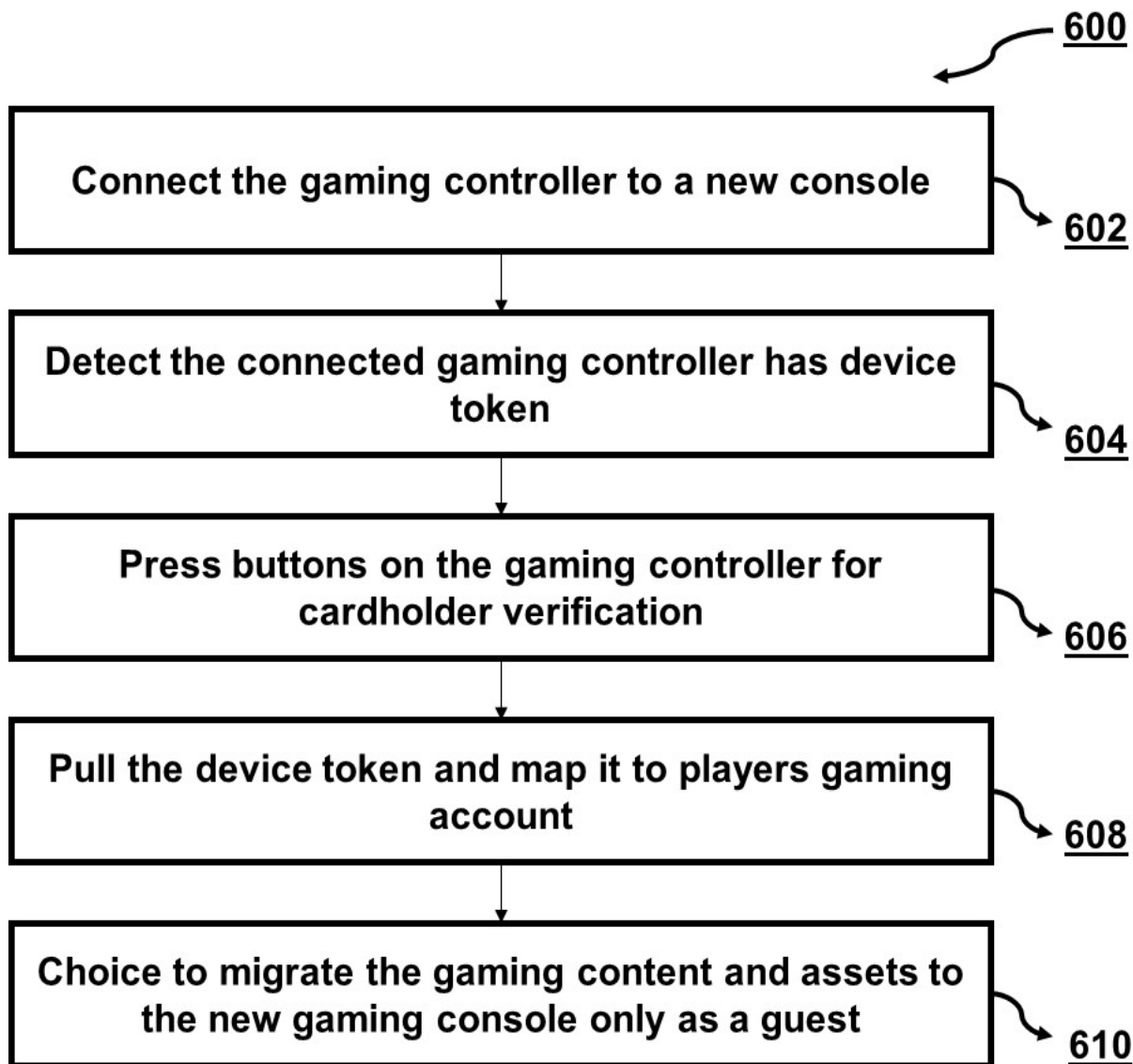


Fig 6