



(12) **DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION**

(13) **A1**

(86) Date de dépôt PCT/PCT Filing Date: 2017/09/20
(87) Date publication PCT/PCT Publication Date: 2018/03/29
(85) Entrée phase nationale/National Entry: 2019/03/20
(86) N° demande PCT/PCT Application No.: US 2017/052454
(87) N° publication PCT/PCT Publication No.: 2018/057592
(30) Priorité/Priority: 2016/09/21 (US62/397,508)

(51) Cl.Int./Int.Cl. *G06Q 20/38* (2012.01),
G06F 21/62 (2013.01), *G06Q 20/34* (2012.01),
G06Q 20/40 (2012.01), *H04L 9/32* (2006.01)
(71) Demandeur/Applicant:
WALMART APOLLO, LLC, US
(72) Inventeurs/Inventors:
JOHNSON, AARON MARCUS, US;
GERBER, CHRISTOPHER JOHN, US;
CORSON, GERALD DUANE, US;
WATTS, CHARLES ALAN, US
(74) Agent: CASSAN MACLEAN IP AGENCY INC.

(54) Titre : SYSTEME ET PROCEDES DE CHIFFREMENT ET DE SEGMENTATION EN UNITES POINT A POINT
(54) Title: SYSTEM AND METHODS FOR POINT TO POINT ENCRYPTION AND TOKENIZATION

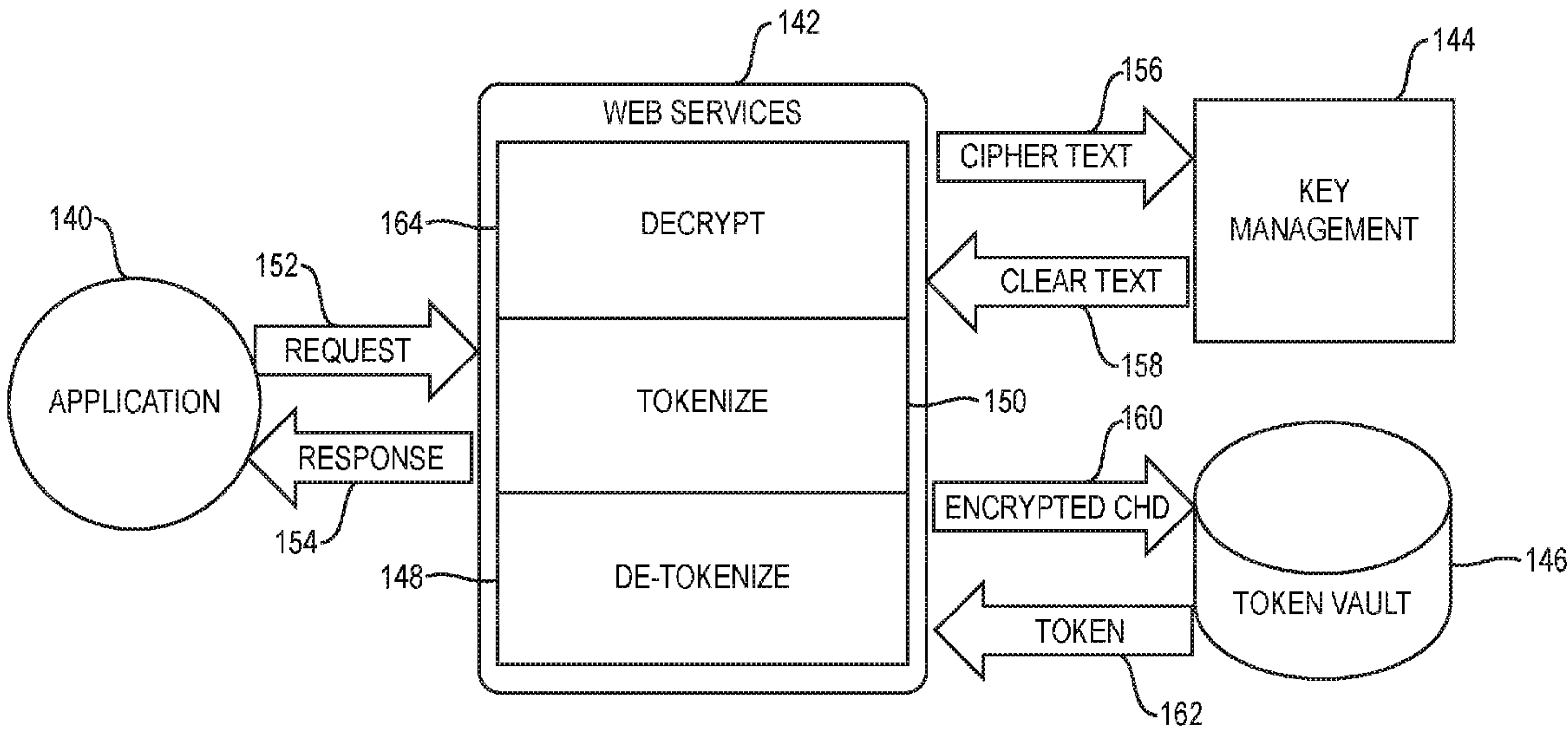


FIG. 1B

(57) **Abrégé/Abstract:**
A system and method for providing point to point encryption and tokenization enabling decryption, tokenization and storage of sensitive encrypted card holder data for payment processing comprising initiated by a pin entry device and comprising encryption and decryption of card holder data and tokens representing card holder data.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
29 March 2018 (29.03.2018)



(10) International Publication Number
WO 2018/057592 A1

(51) International Patent Classification:

G06Q 20/38 (2012.01) *H04L 9/32* (2006.01)
G06Q 20/40 (2012.01) *G06F 21/62* (2013.01)
G06Q 20/34 (2012.01)

(21) International Application Number:

PCT/US2017/052454

(22) International Filing Date:

20 September 2017 (20.09.2017)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/397,508 21 September 2016 (21.09.2016) US

(71) Applicant: **WAL-MART STORES, INC.** [US/US]; 702
Southwest 8th Street, Bentonville, AR 72716 (US).

(72) Inventor; and

(71) Applicant: **JOHNSON, Aaron, Marcus** [US/US]; 905
South 12th Place, Rogers, AR 72756 (US).

(72) Inventors: **GERBER, Christopher, John**; 2 Bytham Cir-
cle, Bella Vista, AR 72714 (US). **CORSON, Gerald, Du-**

ane; 1108 North 37th Street, Rogers, AR 72756 (US).
WATTS, Charles, Alan; 104 Blair Circle, Pea Ridge, AR
72751 (US).

(74) Agent: **BURNS, David, R.** et al.; McCarter & English,
LLP, 265 Franklin Street, Boston, MA 02110 (US).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,

(54) Title: SYSTEM AND METHODS FOR POINT TO POINT ENCRYPTION AND TOKENIZATION

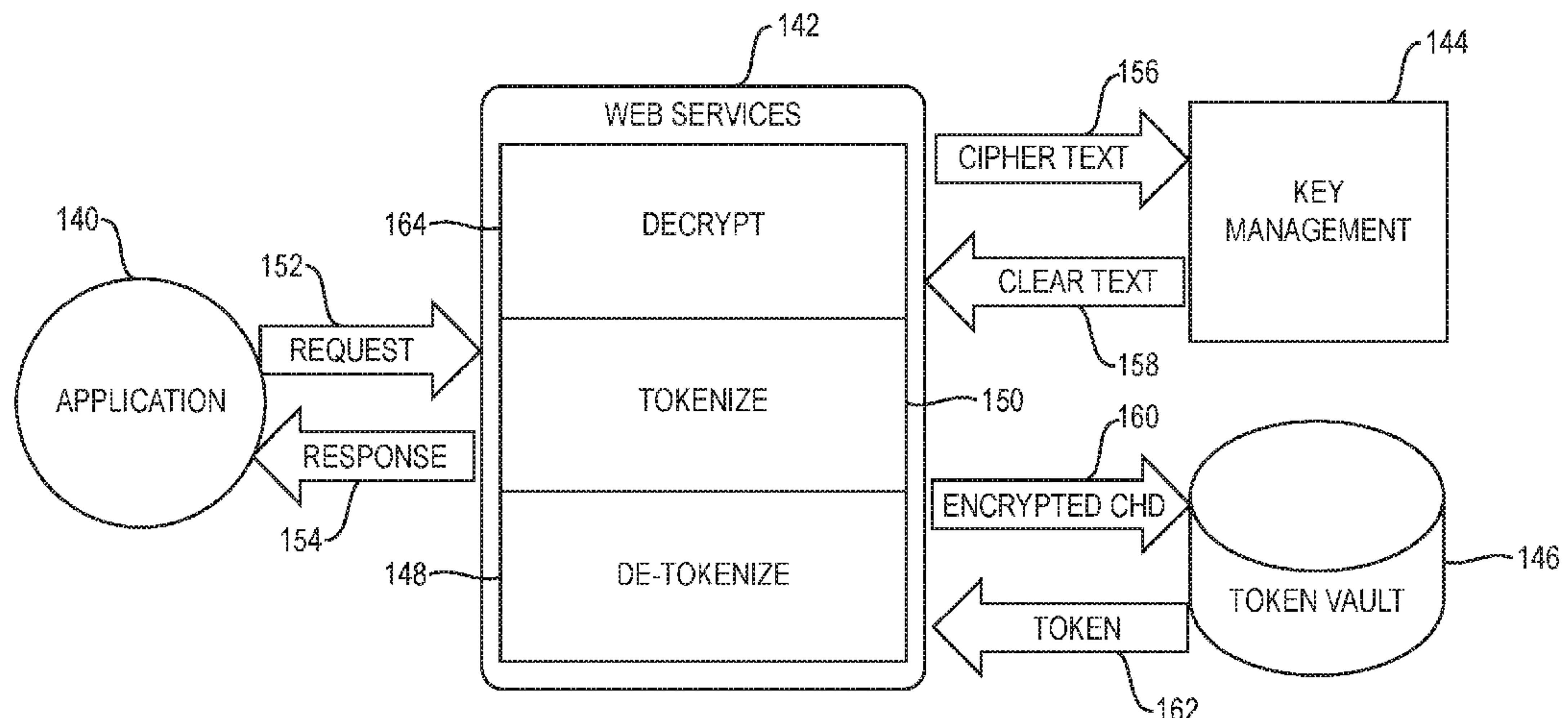


FIG. 1B

(57) Abstract: A system and method for providing point to point encryption and tokenization enabling decryption, tokenization and storage of sensitive encrypted card holder data for payment processing comprising initiated by a pin entry device and comprising encryption and decryption of card holder data and tokens representing card holder data.

[Continued on next page]

WO 2018/057592 A1

EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

SYSTEM AND METHODS FOR POINT TO POINT ENCRYPTION AND TOKENIZATION

CROSS-REFERENCE TO RELATED PATENT APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application No. 62/397,508 filed on September 21, 2016, the content of which is hereby incorporated by reference in its entirety.

BACKGROUND

[0002] Sensitive data may be entrusted to a computing system by a user. The sensitive data may be transferred between different computing systems.

BRIEF SUMMARY

[0003] In one embodiment, a point to point encryption and tokenization system includes a pin entry device (PED) configured to receive and encrypt card holder data (CHD). The system further includes a first computing system in communication with the PED and configured to receive the encrypted CHD. The system further includes a second computing system in communication with the first communication system via a communications network and configured to receive the encrypted CHD from the first communication system. The second computing system includes a decryption module configured to decrypt the CHD, a tokenization module configured to generate a token representing the CHD, an authorization module configured to process the decrypted sensitive data and transmit a confirmation of the processing and the token representing the CHD to the first computing system; and a database in communication configured to store a token representing the decrypted CHD and the decrypted CHD.

[0004] In another embodiment, a method for point to point encryption and tokenization includes receiving and encrypting card holder data (CHD) with a pin entry device (PED) and receiving the encrypted CHD at a first computing system in communication with the PED. The method further includes transmitting the encrypted CHD from the first computing system to the second computing system via a communications network and decrypting the encrypted CHD with a decryption module executing on the second computing system. The method also includes generating a token representing the decrypted CHD with a token module executing on the second computing system, processing the decrypted CHD with an authorization

module executing on the second computing system, transmitting a confirmation of the processing and a copy of the token to the first computing system and storing the token representing the decrypted CHD and the decrypted CHD in a database in communication with the first computing system.

BRIEF DESCRIPTION OF DRAWINGS

[0005] The accompanying figures, which are incorporated in and constitute a part of this specification, illustrate one or more embodiments of the present invention and, together with the description, help to explain the present invention. The embodiments are illustrated by way of example and should not be construed to limit the present invention. In the figures:

[0006] **FIG. 1A** is a block diagram of a point to point encryption and tokenization system in accordance with an exemplary embodiment;

[0007] **FIG. 1B** is a block diagram of data flow in a point to point encryption and tokenization system point in accordance with an exemplary embodiment;

[0008] **FIG. 2** is a network diagram of the point to point encryption and tokenization system according to an exemplary embodiment;

[0009] **FIG. 3** is a block diagram illustrating an exemplary computing device in accordance with an exemplary embodiment;

[0010] **FIG. 4** is a flowchart illustrating an exemplary process performed in a point to point encryption and tokenization system when receiving the encrypted sensitive data for the first time according to an exemplary embodiment; and

[0011] **FIG. 5** is a flowchart illustrating an exemplary process performed in a point to point encryption and tokenization system when receiving the encrypted sensitive data a subsequent time according to an exemplary embodiment.

DETAILED DESCRIPTION

[0012] Embodiments as described herein provide enhanced security to the processing of CHD and other sensitive data in a large-scale payment card data environment by limiting where the data can be accessed. Multiple cryptographic techniques are used to provide data

security. Described in detail herein are point to point encryption and tokenization enabling decryption, tokenization and storage of sensitive encrypted data within a large-scale payment card environment . In one embodiment, sensitive data can be received by a pin entry device (PED). The PED can transmit the encrypted sensitive data to a first computing system for processing the encrypted sensitive data. The first computing system can transmit the encrypted sensitive data to a second computing system for processing the encrypted sensitive data. The second computing system can decrypt the encrypted sensitive data, generate a token representing the decrypted sensitive data and process the decrypted sensitive data. The second computing system can transmit a confirmation of the processing and a copy of the token to the first computing system. The copy of the token can be stored in a database in communication with the first computing system. The second computing system can store the token representing the sensitive decrypted data along with the decrypted data in a database. Subsequently the second computing system can also receive the token from the first computing system as part of a request for processing the decrypted sensitive data from the first computing system. The second computing system can retrieve the decrypted sensitive data associated with the received token and process the decrypted sensitive data in response to the request.

[0013] FIG. 1A is a block diagram of a point to point encryption and tokenization system in accordance with an exemplary embodiment. The point to point encryption and tokenization system 100 can include a PED 134, a first computing system 130, a second computing system 106 and an authorization services system 136. In one embodiment the first computing system 130 can be located in a retail facility 128 and may include a Point-of-Sale (POS) register 130a in communication with a POS controller 130b and the PED 134 can be configured to receive Card Holder Data (CHD) in response to complete a purchase of products. In alternative embodiments, the first computing system 130 and the PED 134 can be disposed in different locations. The first computing system 130 can be connected to the second computing system 106 through a secure network 114. The second computing system 106 can include processing modules connected to each other. In one embodiment, some of the modules may be connected in a Payment Card Industry (PCI) zone 116 configured to process data in compliance with the PCI Data Security Standard (DSS) in a secure environment. The connected processing modules can include a decryption module 120, a tokenization module 122, a web-services module 126 and applications 118. As a non-limiting example, the applications 118 may be one or more of finance, treasury or reconciliation

applications running within a PCI zone. The applications 118 and web services module can be configured to request execution of the decryption module 120 and the tokenization module 122. The second computing system 106 can further include an authorization module 104 and a key management module 102. The key management module 102 can include a certificate authority server 112 and a public key server 110. The decryption module 120, tokenization module 112, authorization module, and key management module 102 each can be segmented into different zones within the second computing system 106 to ensure that each module is able to communicate with one another only when necessary and authorized. In this configuration the segmented zones cannot access data from another segmented zone unless permission is granted. Each of the segmented zones provide a layer of security. For example, the layer of security can be a combination of one or more of: access control lists which limit which IP addresses can communicate with one another via TCP/UDP ports, firewalls which can provide similar functionality to the access control lists but also may perform stateful packet and application inspection and intrusion prevention systems which monitor network behavior for malicious activity and blocks based on policies. The security layers ensure the data is protected when being transferred from one segmented zone to the other within the second computing system 106. It will be appreciated that additional layers of security and/or techniques may also be deployed by the second computing system without departing from the scope of the present invention.

[0014] In one embodiment, the PED 134 can receive and encrypt sensitive data. For example, the PED 134 may receive and encrypt credit card data. In one embodiment the PED 134 can use asymmetric encryption to encrypt the sensitive data. Asymmetric encryption is a form of encryption in which keys are generated in pairs. The sensitive data can be encrypted using a first key and decrypted using a different second key. In another embodiment, the PED 134 may use symmetric encryption to encrypt and decrypt the sensitive data where copies of the same key are used for encryption and decryption. The encrypted sensitive data can be transmitted to the first computing system 130. The first computing system 130 can transmit the encrypted sensitive data 130 for processing to the second computing system 106. The first computing system 130 can also send a security certificate with the encrypted sensitive data to the second computing system. The authorization module 104 can receive the encrypted sensitive data and the security certificate and transmit the encrypted sensitive data and the security certificate to the web-services module 126 for further handling. The web-services module 126 can attempt authentication of the encrypted sensitive data by transmitting the

security certificate to the certificate authority server 112. The certificate authority server 112 can authenticate the security certificate and transmit a confirmation of authentication to the web-services module 126. The web-services module 126 can then route the encrypted sensitive data to the decryption module 120.

[0015] In one embodiment, the decryption module 120 can be a Hardware Security Module (HSM). A HSM is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto-processing. The decryption module 120 can decrypt the sensitive data. The decryption module 120 can retrieve a public key to decrypt the encrypted sensitive data from the public key server 110. The decryption module 120 transmits the decrypted sensitive data to the web-services module 126. The web-services module 126 can route the decrypted sensitive data to the tokenization module 122. The tokenization module 122 can generate a token using tokenization. Tokenization is the process of substituting sensitive data with a non-sensitive equivalent. For example, the token can be an alphanumeric string that is different from the decrypted sensitive data and represent the decrypted sensitive data. The tokenization module 122 can store the token and the decrypted sensitive data in a token vault. The tokenization module 122 can transmit the token to the web-service module 122 along with the decrypted sensitive data. The web-services module 122 can transmit the decrypted sensitive data and the token to the authorization module 104 for further processing. The authorization module 136 can transmit the decrypted sensitive data to authorization services 136 to complete an authorization process using the decrypted data. In one embodiment, the authorization services 136 can be located outside of the second computing system and, for example, if run by a third party, the decrypted data can re-encrypted for transit and then decrypted again by the authorization services so that authorization can be performed. The authorization services 136 can process the sensitive data and transmit a confirmation of processing to the authorization module 104. The authorization module 104 can transmit a receipt of completion of the processing along with the token representing the decrypted sensitive data to the first computing system 130. The first computing system 130 can store the token in a transaction log in a database instead of storing the sensitive data itself.

[0016] The first computing system 130 can receive a request to process the same encrypted sensitive data a subsequent time. For example, this could occur when the first computing system 130 receives a request from a user to perform a transaction using saved card data.

The first computing system 130 can transmit the token associated with the encrypted sensitive data from the transaction log to the second computing system 106 as part of a request. The authorization module 104 can receive the token and transmit the token to the web-services module 126. The web-services module 126 can retrieve the decrypted sensitive data associated with the token. The web-services module 126 can transmit the decrypted sensitive data associated to the authorization module 104 and the authorization module 104 can transmit the sensitive decrypted sensitive data to the authorization services 136. The authorization services 136 can authorize the decrypted sensitive data and transmit a confirmation to the authorization module 104. The authorization module 104 can transmit a receipt confirming authorization processing along with the token to the first computing system 130. In this manner sensitive data can be referenced at the first computing system without actually being present thus enhancing security.

[0017] FIG. 1B is a block diagram of data flow in a point to point encryption and tokenization system point in accordance with an exemplary embodiment. web-services module 142 can be implemented as middleware within the second computing system. In one embodiment, the web services module 142 may provide some or all of the services using a representational state transfer (REST) architecture (i.e. the services may be RESTful services) The web-services module 142 can receive a request 152 from an application 140 to process sensitive data. In the event the request includes encrypted sensitive data, the web services module can utilize the decryption module 164 to decrypt the encrypted sensitive data. The decryption module 164 can transmit the encrypted sensitive data to the key management module 144 as cipher text 156 and the key management module 144, may decrypt the encrypted sensitive data and transmit the decrypted sensitive data as clear text 158 to the web-services module 142. The web-services module 142 can transmit the decrypted sensitive data to the tokenization module 150 so that the tokenization module 150 can generate a token to represent the decrypted sensitive data. The tokenization module 150 can transmit the decrypted sensitive data 160 and token to a token vault 146 for storage. The web-services module 142 can process the request 152 and transmit a response 154 back to the application 140. For example, the response may indicate that a transaction has been authorized.

[0018] In the event the web-services module 142 receives a token in the request to process sensitive data the web-services module 142 can transmit the token to the de-tokenization

module 148. The detokenization module 148 can access the decrypted sensitive data in the token vault 146 using the token to find the associated data.. The web-services module 142 can process the decrypted sensitive data and transmit a response 154 from processing the decrypted sensitive data back to the application 140.

[0019] FIG. 2 illustrates an exemplary point to point encryption and tokenization system 255. The point encryption and tokenization system 255 can include a first database 205, a second database 207, one or more of first computing systems 200, one or more of the second computing systems 250, one or more mobile devices 260 and one or more pin entry devices 245. In one exemplary embodiment, the first computing system 200 can be in communication with the first database(s) 205, the mobile devices 260, and the pin entry devices 245, via a first communications network 215. The second computing system 250 can be in communication with the second database(s) 207, and the first computing system 200, via second communication network 217.

[0020] In an example embodiment, one or more portions of the first and second communications network 215, 217 can be an ad hoc network, an intranet, an extranet, a virtual private network (VPN), a local area network (LAN), a wireless LAN (WLAN), a wide area network (WAN), a wireless wide area network (WWAN), a metropolitan area network (MAN), a portion of the Internet, a portion of the Public Switched Telephone Network (PSTN), a cellular telephone network, a wireless network, a WiFi network, a WiMax network, any other type of network, or a combination of two or more such networks.

[0021] The first computing system 200 may include one or more computers or processors configured to communicate with first database(s) 205, the mobile devices 260, and the pin entry devices 245, via the first network 215. The first computing system 200 may host one or more applications configured to interact with one or more components first computing system 200 and/or facilitates access to the content of the first databases 205. The second computing system 250 includes one or more computers or processors configured to communicate with the second database(s) 207, and the first computing system 200, via second communication network 217. The second computing system 250 may host one or more applications configured to interact with one or more components of the first computing system 200 and/or facilitates access to the content of the second databases 207. The first databases 205 may store information/data, as described herein. For example, the first databases 205 can include a physical objects database 240. The physical objects database 240 can store information

associated with physical objects disposed at various facilities . The first databases 205 can be located at one or more geographically distributed locations from each other or from the first computing system 200. Alternatively, the first databases 205 can be included within in a computer or processing device of the first computing system 200. The second databases 207 may store information/data, as described herein. For example, the second databases 207 can include a token vault. The token vault 235 can store sensitive decrypted data and a token representing the sensitive decrypted data. The second databases 207 can be located at one or more geographically distributed locations from each other or from the second computing system 250. Alternatively, the second databases 207 can be included within a computer or processing device of the second computing system 250.

[0022] As a non-limiting example, the point encryption and tokenization system 255 can be implemented in a physical retail store. In another embodiment, a mobile device 260 can receive CHD for completing a purchase on an online retail store using a mobile application. The mobile device 260 can encrypt the CHD using asymmetric encryption and transmit the encrypted CHD to a first computing system 200. . In some embodiments, the mobile device 260 and the first computing system 200 can be in different geographic locations. In other embodiments, the mobile device 260 and the first computing system 200 can be in the same geographic location.

[0023] Once the encrypted CHD is received, the first computing system 200 can transmit the encrypted CHD for processing a payment to the second computing system 250, via the second network 217. The first computing system 200 can also send a security certificate along with the encrypted CHD. An authorization module (e.g. authorization module 104 as shown in **FIG. 1A**) in the second computing system 250 can receive the encrypted CHD and the security certificate and transmit the encrypted CHD and the security certificate to the web-services module (e.g. web-services module 126 and 142 as shown in **FIG. 1A-B**) in the second computing system 250. The web-services module can authenticate the encrypted CHD by transmitting the security certificate to a certificate authority server (e.g. certificate authority server 112 as shown in **FIG. 1A**) within the second computing system 250. The certificate authority server can authenticate the security certificate and transmit a confirmation of authentication to the web-services module. The web-services module can then route the encrypted CHD to the decryption module (e.g. decryption module 120 and 164 as shown in **FIG. 1A-B**) within the second computing system 250.

[0024] The decryption module can be a Hardware Security Module (HSM). The decryption module can decrypt the encrypted CHD. The decryption module can retrieve the public key needed to decrypt the encrypted CHD from a public key server (e.g. public key server 110 or key management module 144 as shown in **FIG. 1A-B**). For example, the public key can be embodied . The decryption module may transmit the decrypted CHD to the web-services module. The web-services module can route the decrypted CHD to the tokenization module (e.g. tokenization module 122 and 150 as shown in **FIG. 1A-B**). The tokenization module can generate a token representing the decrypted CHD. The tokenization module can store the token and the decrypted CHD in a token vault 245. The tokenization module can transmit the token to the web-service module along with the decrypted CHD. The web-services module can then transmit the decrypted CHD and the token to the authorization module. The authorization module can transmit the decrypted CHD to the authorization services (e.g. authorization services 136 as shown in **FIG. 1A**). The authorization services 136 can be outside of the second computing system (in which case the decrypted CHD may be re-encrypted for transit) and can be configured to process payment information using the CHD and to transmit a confirmation of payment processing to the authorization module. The authorization module can transmit a receipt of payment (indicating a transaction was successfully processed) along with the token representing the decrypted CHD to the first computing system 200. The first computing system 200 can store the token in a transaction log.

[0025] The first computing system 200 can subsequently receive a request to process the same encrypted CHD a subsequent time. For example, a request may be received from a user to conduct a transaction using stored card data. The first computing system 200 can determine that there is a token associated with the encrypted CHD. The first computing system 200 can retrieve the token associated with the encrypted CHD from a transaction log, for example from a transaction log stored in a database in communication with the first computing system, and transmit the token to the second computing system 250 in order to have a transaction authorized. The authorization module can receive the token and transmit the token to the web-services module. The web-services module can retrieve the decrypted CHD associated with the token from the token vault 235 using the token. The web-services module can transmit the decrypted CHD associated to the authorization module. The authorization module can transmit the decrypted CHD to the authorization services. The authorization service can authorize and process the payment information using the CHD and

transmit a confirmation of the payment to the authorization module. The authorization module can then transmit a receipt payment with the token to the first computing system 200.

[0026] As a non-limiting example, an encrypted CHD can be embodied as:

f17mcS9Ct+hosrfN/gzl3Jaqy3nsZF5GU0lAMAS00DNbiiGqTI3GLYG/rQZfM6AZqRfw4q
RuydhskHv3KdUgrMi2PyW8QobtdGaP837n5uwKTAZAFuRnMGpATk44pwUdF09RJWH
dRpIMEOAqfX0AaqcnUIHZq6ncXHNZakSrhYwDyONV8fwIWdhs8T2KEEi+vYkOck9ip
Sy34XX/TLzDVhEyHLxfpDgb2er9EmOAsOsmFJgldVRHJA9XtLPEoyqpx6EWakCB/ZMp
6CYV28WbADtoavnk6GIroICxb1QTTGwYv7CzEG014hs81KiU3crin7HCsMEN3oMW7p
PEMKa/4w==. An public key to decrypt the encrypted CHD can be embodied as:
as:b5acf232rf3 . A token generated for the CHD can be embodied as:
rZMW2fymN4Huk9gGHCFTi9AQHxX62biXSeframpbefo=.

[0027] FIG. 3 is a block diagram of an example computing device for implementing exemplary embodiments. The computing device 300 can implement embodiments of the first computing system, the second computing system, the PED, and the mobile device. The computing device 300 includes one or more non-transitory computer-readable media for storing one or more computer-executable instructions or software for implementing exemplary embodiments. The non-transitory computer-readable media may include, but are not limited to, one or more types of hardware memory, non-transitory tangible media (for example, one or more magnetic storage disks, one or more optical disks, one or more flash drives, one or more solid state disks), and the like. For example, memory 306 included in the computing device 300 may store computer-readable and computer-executable instructions or software (e.g., applications 330) for implementing exemplary operations of the computing device 300. The computing device 300 also includes configurable and/or programmable processor 302 and associated core(s) 304, and optionally, one or more additional configurable and/or programmable processor(s) 302' and associated core(s) 304' (for example, in the case of computer systems having multiple processors/cores), for executing computer-readable and computer-executable instructions or software stored in the memory 306 and other programs for implementing exemplary embodiments. Processor 302 and processor(s) 302' may each be a single core processor or multiple core (304 and 304') processor. Either or both of processor 302 and processor(s) 302' may be configured to execute one or more of the instructions described in connection with computing device 300.

[0028] Virtualization may be employed in the computing device 300 so that infrastructure and resources in the computing device 300 may be shared dynamically. A virtual machine 312 may be provided to handle a process running on multiple processors so that the process appears to be using only one computing resource rather than multiple computing resources. Multiple virtual machines may also be used with one processor.

[0029] Memory 306 may include a computer system memory or random access memory, such as DRAM, SRAM, EDO RAM, and the like. Memory 306 may include other types of memory as well, or combinations thereof.

[0030] A user may interact with the computing device 300 through a visual display device 314, such as a computer monitor, which may display one or more graphical user interfaces 316, multi touch interface 320, a pointing device 318, an scanner 336 and a reader 332. The scanner 336 and reader 332 can be configured to read sensitive data.

[0031] The computing device 300 may also include one or more storage devices 326, such as a hard-drive, CD-ROM, or other computer readable media, for storing data and computer-readable instructions and/or software that implement exemplary embodiments (e.g., applications). For example, exemplary storage device 326 can include one or more databases 328 for storing information regarding available physical objects and account holder information. The databases 328 may be updated manually or automatically at any suitable time to add, delete, and/or update one or more data items in the databases.

[0032] The computing device 300 can include a network interface 308 configured to interface via one or more network devices 324 with one or more networks, for example, Local Area Network (LAN), Wide Area Network (WAN) or the Internet through a variety of connections including, but not limited to, standard telephone lines, LAN or WAN links (for example, 802.11, T1, T3, 56kb, X.25), broadband connections (for example, ISDN, Frame Relay, ATM), wireless connections, controller area network (CAN), or some combination of any or all of the above. In exemplary embodiments, the computing system can include one or more antennas 322 to facilitate wireless communication (e.g., via the network interface) between the computing device 300 and a network and/or between the computing device 300 and other computing devices. The network interface 308 may include a built-in network adapter, network interface card, PCMCIA network card, card bus network adapter, wireless network adapter, USB network adapter, modem or any other device suitable for interfacing the

computing device 300 to any type of network capable of communication and performing the operations described herein.

[0033] The computing device 300 may run operating system 310, such as versions of the Microsoft® Windows® operating systems, different releases of the Unix and Linux operating systems, versions of the MacOS® for Macintosh computers, embedded operating systems, real-time operating systems, open source operating systems, proprietary operating systems, or other operating systems capable of running on the computing device 300 and performing the operations described herein. In exemplary embodiments, the operating system 310 may be run in native mode or emulated mode. In an exemplary embodiment, the operating system 310 may be run on one or more cloud machine instances.

[0034] **FIG. 4** is a flowchart illustrating an exemplary process performed in a point to point encryption and tokenization system when receiving encrypted sensitive data for the first time according to an exemplary embodiment. In operation 400, a PED (e.g. PED 134 and 245 as shown in **FIGS. 1A and 2**) or mobile device (e.g. mobile device 260 as shown in **FIG. 2**) can receive CHD or other sensitive data for processing. In one embodiment, the PED or mobile device can encrypt the data using asymmetric encryption. In operation 402, the PED or mobile device can transmit the encrypted CHD or other sensitive data to the first computing system (e.g. first computing system 134 and 200 as shown in **FIGS. 1A and 2**).

[0035] In operation 404, the first computing system can transmit the encrypted CHD or other sensitive data to the second computing system (e.g. second computing system 106 and 250 as shown in **FIGS. 1A and 2**). The first computing system can also send a security certificate along with the encrypted data. In operation 406, the second computing system decrypts the encrypted CHD or other sensitive data following authentication. For example, an authorization module (e.g. authorization module 104 as shown in **FIG. 1A**) in the second computing system can receive the encrypted CHD or other sensitive data and the security certificate and transmit the encrypted CHD or other sensitive data and the security certificate to the web-services module (e.g. web-services module 126 and 142 as shown in **FIG. 1A-B**) within the second computing system. The web-services module can authenticate the encrypted CHD or other sensitive data by transmitting the security certificate to the certificate authority server (e.g. certificate authority server 112 as shown in **FIG. 1A**) within the second computing system 250. The certificate authority server can authenticate the security certificate and transmit a confirmation of authentication to the web-services module.

The web-services module can then route the encrypted sensitive data to the decryption module (e.g. decryption module 120 and 164 as shown in **FIG. 1A-B**) within the second computing system for decryption.

[0036] The decryption module can be a Hardware Security Module (HSM) configured to decrypt the encrypted CHD or other sensitive data. For example, the decryption module can retrieve a public key to decrypt the encrypted CHD or other sensitive data from the public key server (e.g. public key server 110 or key management module 144 as shown in **FIG. 1A-B**). The decryption module then transmit the decrypted CHD or other sensitive data to the web-services module which in turn may route the decrypted CHD or other sensitive data to the tokenization module (e.g. tokenization module 122 and 150 as shown in **FIG. 1A-B**). In operation 408, the tokenization module can generate a token representing the decrypted CHD or other sensitive data. The tokenization module can store the token and the decrypted CHD or other sensitive data in a token vault (e.g. token vault 245 as shown in **FIG. 2**). The tokenization module can then transmit the token to the web-service module along with the decrypted CHD or other sensitive data for routing to an authorization module to perform the requested authorization processing.. In operation 410 the authorization module may process the decrypted CHD or other sensitive data according to the request of the first computing system., For example, the authorization module may transmit the decrypted sensitive data to authorization services (e.g. authorization services 136 as shown in **FIG. 1A**) to determine whether a payment should be authorized form a user's account. In one embodiment, the authorization services can be located outside of the second computing system and the decrypted CHD or other sensitive data may be re-encrypted for transit to the authorization services. For example, the authorization services may be a third party payment processing system. The authorization services may process the CHD or other sensitive data and transmit a confirmation of processing back to the authorization module. In operation 412, the authorization module can transmit a receipt or other confirmation of the processing along with the token representing the decrypted CHD or other sensitive data to the first computing system. The first computing system can store the token for future reference, for example, such as by storing the token in a transaction log or other storage location in a database.

[0037] **FIG. 5** is a flowchart illustrating an exemplary process performed in a point to point encryption and tokenization system when receiving the encrypted sensitive data a subsequent time according to an exemplary embodiment. In operation 500, the first computing system

(e.g. first computing system 134 and 200 as shown in **FIGS. 1A and 2**) can receive a request to process the encrypted sensitive data a subsequent time. For example, a user may wish to rely on data that has already been provided to the first computing system. The first computing system can determine that there is a token associated with the encrypted sensitive data. In operation 502, the first computing system can retrieve the token associated with the encrypted sensitive data. For example, the token may be retrieved from a transaction log holding information regarding previous transactions. In operation 504, the first computing system can transmit the token associated with the encrypted sensitive data to the second computing system (e.g. second computing system 106 and 250 as shown in **FIGS. 1A and 2**). In operation 506, the authorization module (e.g. authorization module 104 as shown in **FIG. 1A**) can receive the token and transmit the token to the web-services module. In operation 508, the web-services module can retrieve the decrypted sensitive data associated with the token from the token vault (e.g. token vault 245 as shown in **FIG. 2**) using the token.

[0038] In operation 510, the web-services module can transmit the decrypted sensitive data associated to the authorization module. In operation 512, the authorization module can transmit the sensitive decrypted sensitive data to the authorization module (e.g. authorization services 136 as shown in **FIG. 1A**). The authorization services can process and authorize the decrypted sensitive data and transmit a confirmation to the authorization module. In operation 514, the authorization module can transmit a receipt of processing the decrypted sensitive data accompanied by the token to the first computing system.

[0039] In describing exemplary embodiments, specific terminology is used for the sake of clarity. For purposes of description, each specific term is intended to at least include all technical and functional equivalents that operate in a similar manner to accomplish a similar purpose. Additionally, in some instances where a particular exemplary embodiment includes a plurality of system elements, device components or method steps, those elements, components or steps may be replaced with a single element, component or step. Likewise, a single element, component or step may be replaced with a plurality of elements, components or steps that serve the same purpose. Moreover, while exemplary embodiments have been shown and described with references to particular embodiments thereof, those of ordinary skill in the art will understand that various substitutions and alterations in form and detail may be made therein without departing from the scope of the present invention. Further still,

other aspects, functions and advantages such as different combinations of the described embodiments are also within the scope of the present invention.

[0040] Exemplary flowcharts are provided herein for illustrative purposes and are non-limiting examples of methods. One of ordinary skill in the art will recognize that exemplary methods may include more or fewer steps than those illustrated in the exemplary flowcharts, and that the steps in the exemplary flowcharts may be performed in a different order than the order shown in the illustrative flowcharts.

We Claim:

1. A point to point encryption and tokenization system, comprising:
 - a pin entry device (PED) configured to receive and encrypt card holder data (CHD);
 - a first computing system in communication with the PED and configured to receive the encrypted CHD;
 - a second computing system in communication with the first communication system via a communications network and configured to receive the encrypted CHD from the first communication system, the second computing system including:
 - a decryption module configured to decrypt the CHD,
 - a tokenization module configured to generate a token representing the CHD,
 - an authorization module configured to process the decrypted CHD and transmit a confirmation of the processed decrypted CHD and the token representing the CHD to the first computing system; and
 - a database configured to store a token representing the decrypted CHD and the decrypted CHD.
2. The system of claim 1, wherein the second computing system is further configured to:
 - receive a request from the first computing system for an operation on decrypted CHD, the request accompanied by the token;
 - receive the token representing the decrypted CHD at the tokenization module;
 - retrieve the decrypted CHD using the token; and
 - process the operation using the decrypted CHD.
3. The system of claim 2, wherein the decryption module is a Hardware Security Module (HSM).
4. The system of claim 1 wherein the first computing system is further configured to:
 - receive an authorization from the authorization module and store a token representing the CHD in a transaction log.
5. The system of claim 1, wherein the first computing system and the second computing system are located in different geographic locations.

6. The system of claim 1, wherein the CHD is encrypted using asymmetric encryption.
7. The system of claim 1, wherein the second computing system further comprising a key management system configured to issue public keys and store security certificates.
8. The system of claim 1, wherein the decrypted CHD is in a first format, the encrypted CHD is in a second format and the token representing the decrypted CHD is in a third format.
9. The system of claim 1, wherein the token is an alphanumeric string.
10. A point to point encryption and tokenization method, comprising:
 - receiving and encrypting card holder data (CHD) with a pin entry device (PED);
 - receiving the encrypted CHD at a first computing system in communication with the PED;
 - transmitting the encrypted CHD from the first computing system to the second computing system via a communications network;
 - decrypting the encrypted CHD with a decryption module executing on the second computing system;
 - generating a token representing the decrypted CHD with a token module executing on the second computing system;
 - processing the decrypted CHD with an authorization module executing on the second computing system;
 - transmitting, a confirmation of the processed decrypted CHD and a copy of the token to the first computing system; and
 - storing the token representing the decrypted CHD and the decrypted CHD in the database.
11. The method of claim 10, further comprising,
 - receiving, via the second computing system, a request from the first computing system for processing of the decrypted CHD, the request accompanied by the token;
 - receiving the token representing the decrypted CHD at the tokenization module;

retrieving, via the tokenization module, the decrypted CHD using the token; and
processing, via the authentication module, the decrypted CHD.

12. The method of claim 11, wherein the decryption module is a Hardware Security Module (HSM).
13. The method of claim 10, wherein the first computing system and the second computing system are located in different geographic locations.
14. The method of claim 10, wherein the CHD is encrypted using asymmetric encryption.
15. The method of claim 10, wherein the second computing system includes a key management system configured to issue public keys and store security certificates.
16. The method of claim 10, wherein the decrypted CHD is in a first format, the encrypted CHD is in a second format and the token representing the decrypted CHD is in a third format.
17. The method of claim 10, wherein the token is an alphanumeric string.
18. A non-transitory computer readable memory medium storing instructions, wherein the instructions are executable by a processor to:
 - receive and encrypting card holder data (CHD) with a pin entry device (PED);
 - receive the encrypted CHD at a first computing system in communication with the PED;
 - transmit the encrypted CHD from the first computing system to the second computing system via a communications network;
 - decrypt the encrypted CHD with a decryption module executing on the second computing system;
 - generate a token representing the decrypted CHD with a token module executing on the second computing system;
 - process the decrypted CHD with an authorization module executing on the second computing system;

transmit, a confirmation of the processed decrypted CHD and a copy of the token to the first computing system; and

store the token representing the decrypted CHD and the decrypted CHD in the database.

19. The non-transitory computer readable memory medium in claim 17, further comprising,

receive, via the second computing system, a request from the first computing system for processing of the decrypted CHD, the request accompanied by the token;

receive the token representing the decrypted CHD at the tokenization module;

retrieve, via the tokenization module, the decrypted CHD using the token; and

process, via the authentication module, the decrypted CHD.

20. The non-transitory computer readable memory medium in claim 18, wherein the decryption system is a Hardware Security Module (HSM).

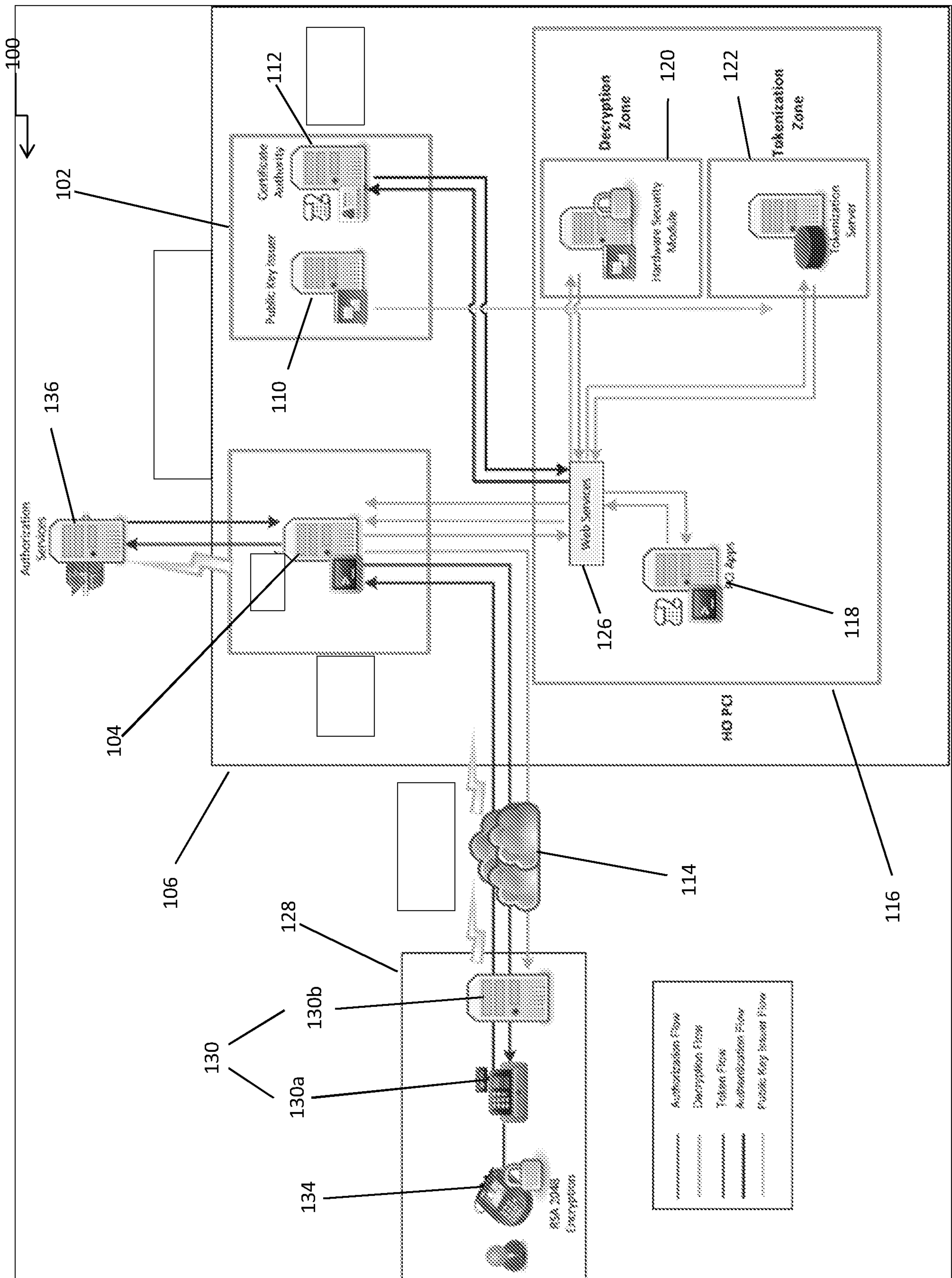


FIG. 1A

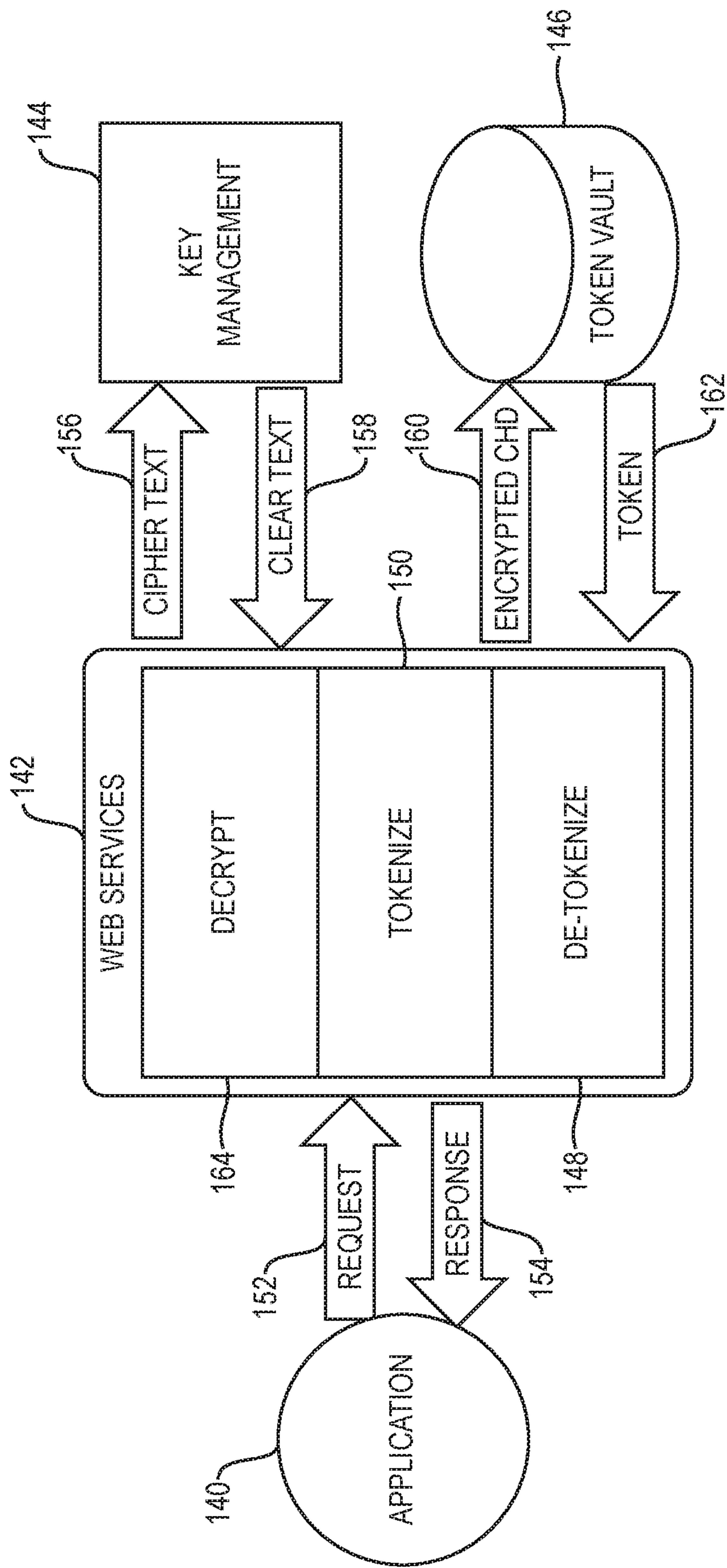


FIG. 1B

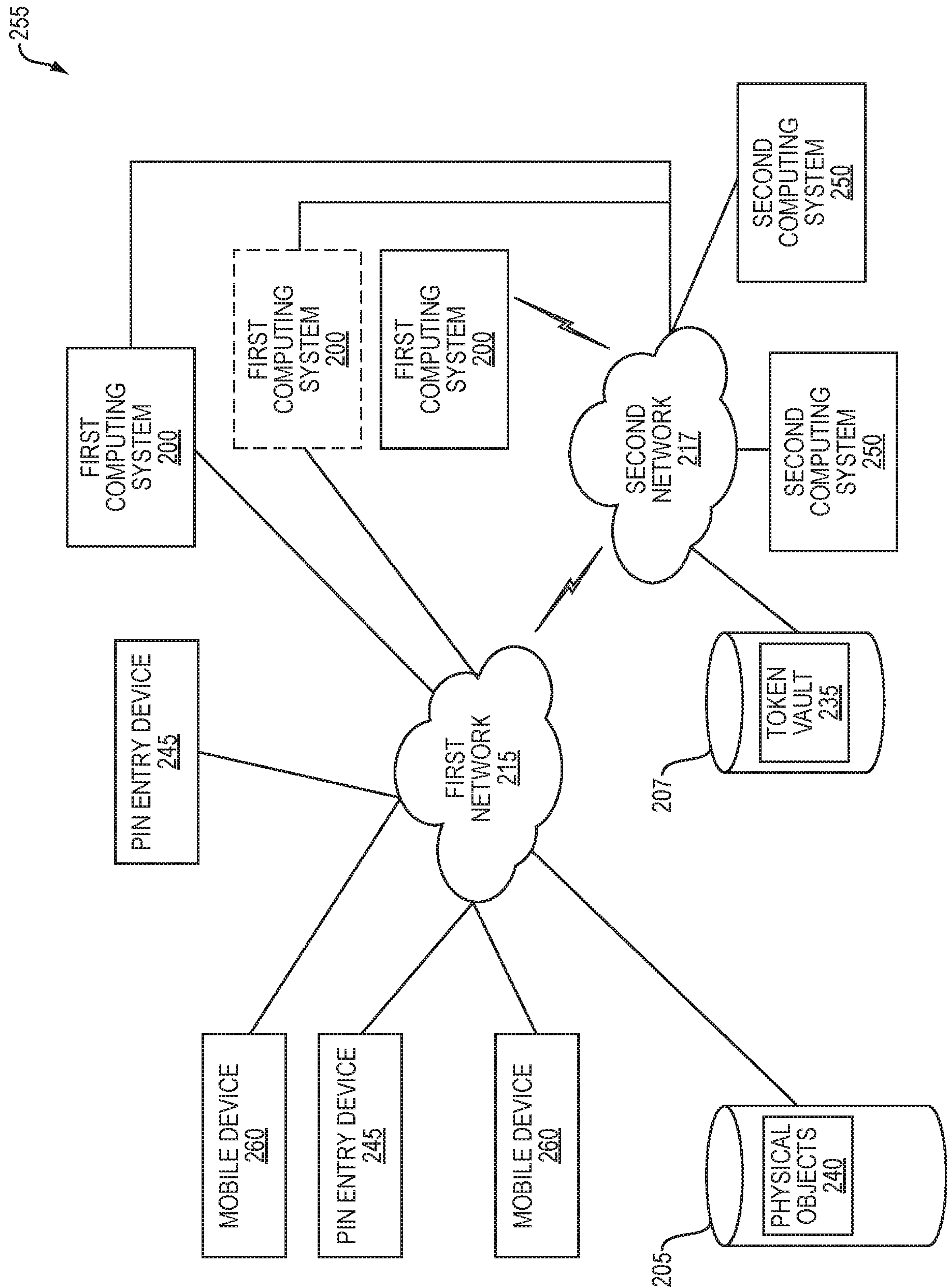


FIG. 2

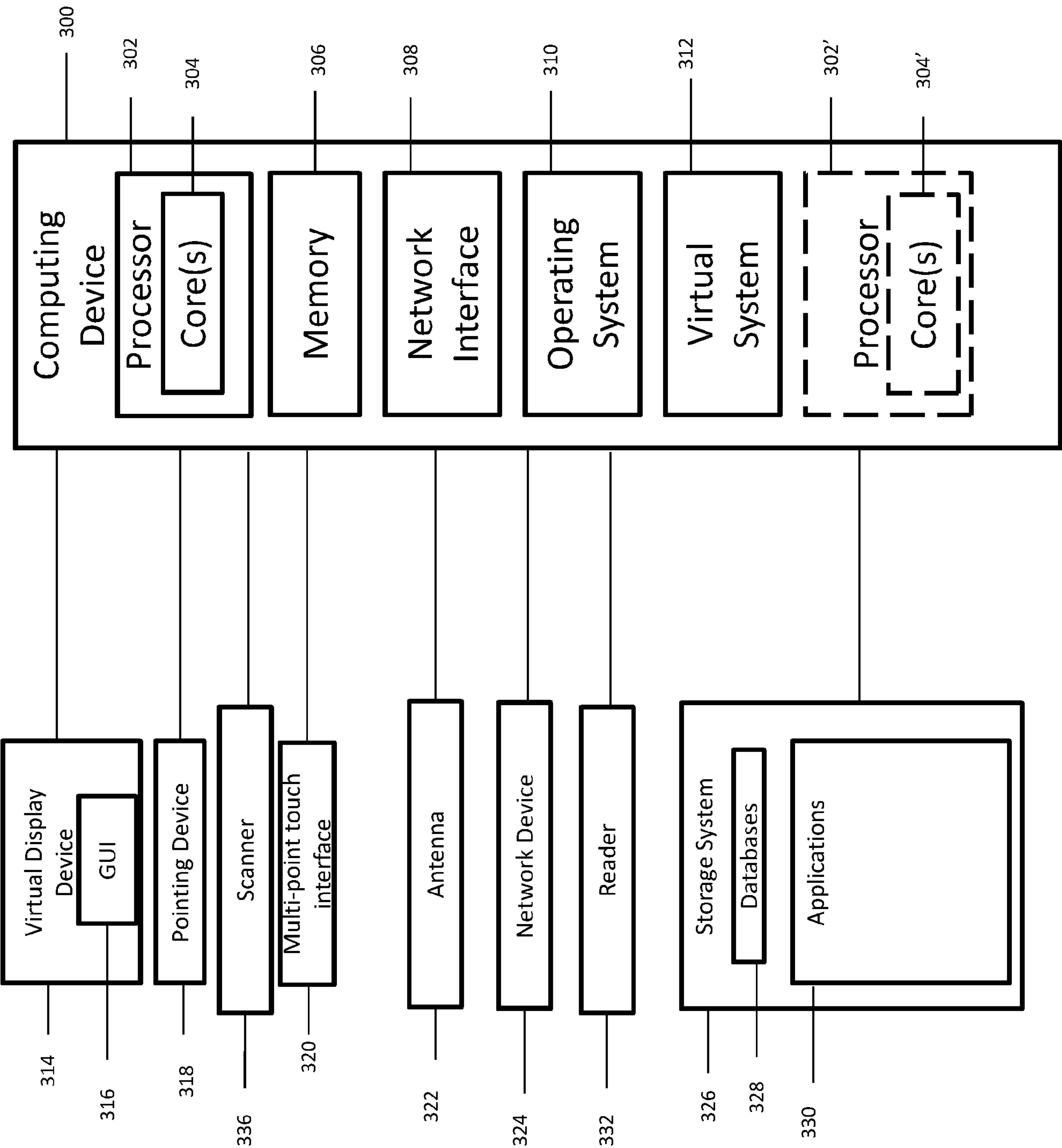


FIG. 3

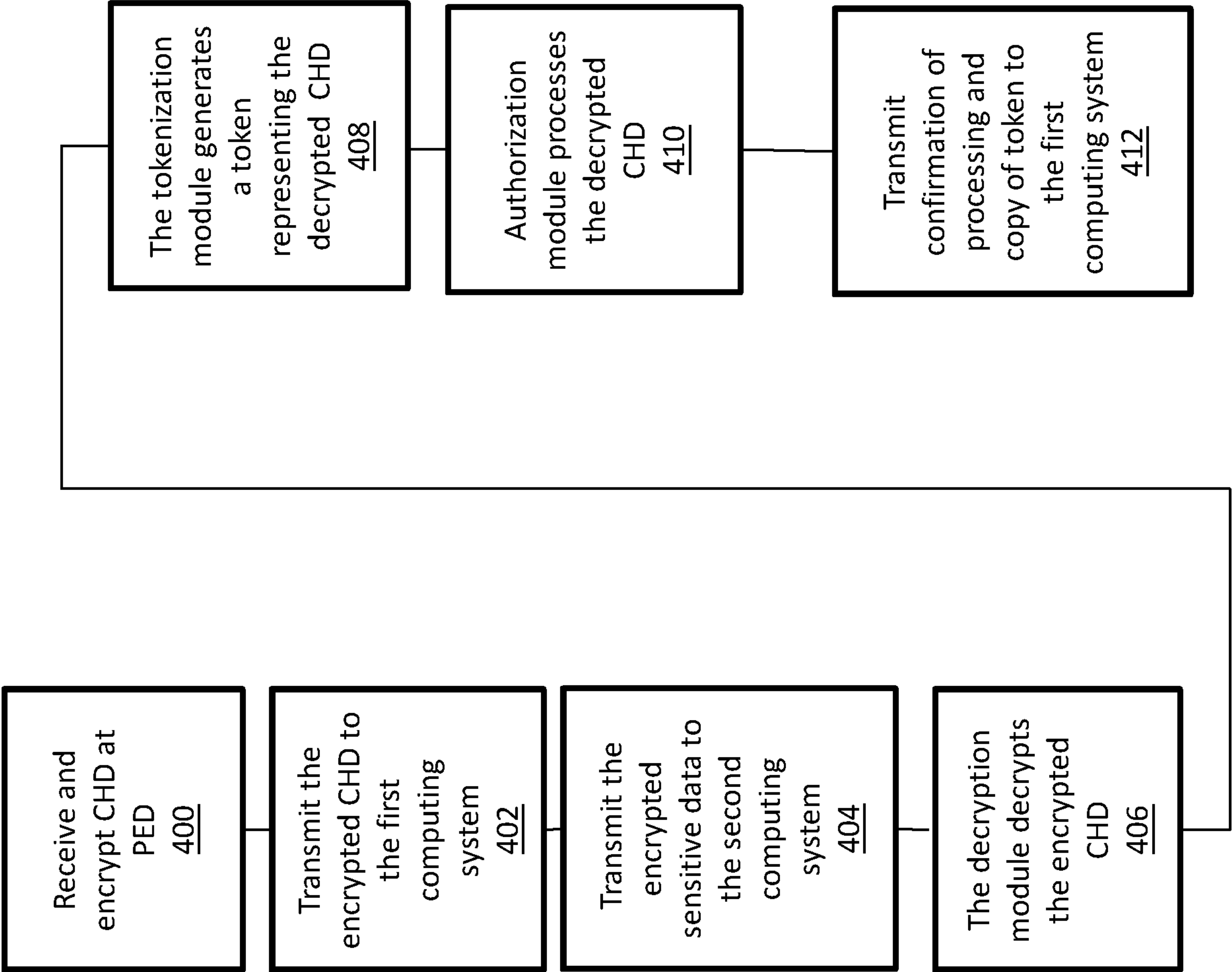


FIG. 4

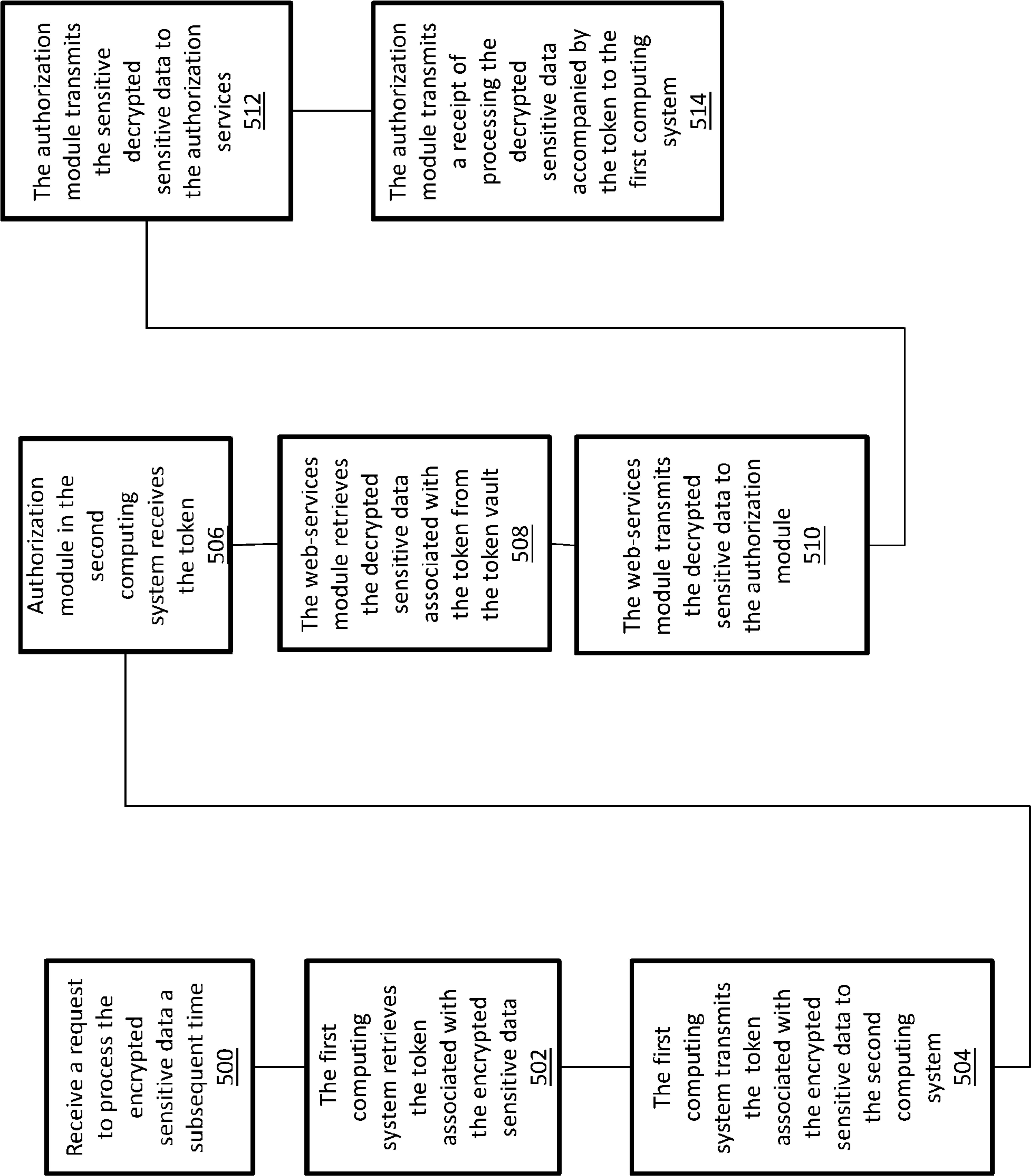


FIG. 5

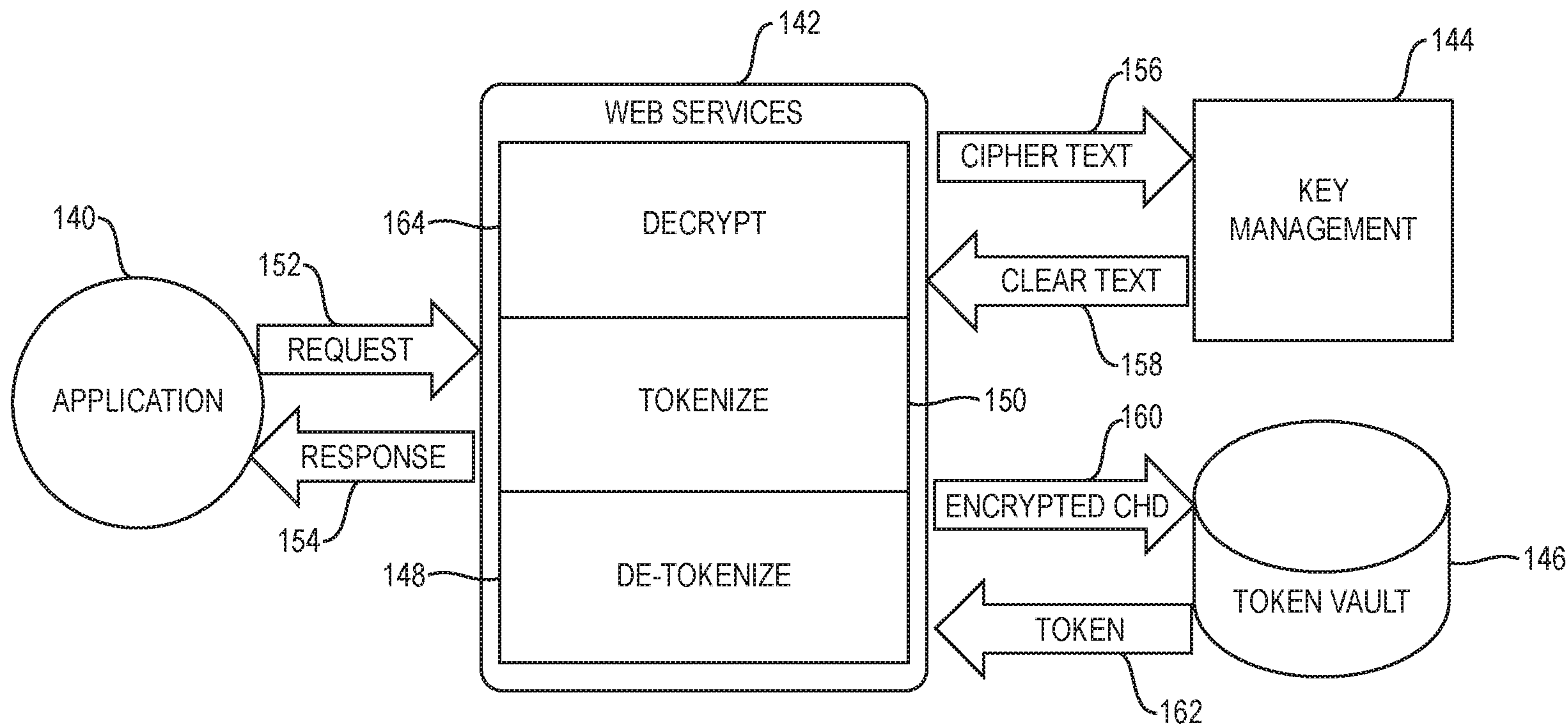


FIG. 1B