(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)

WIPO | PCT

(10) International Publication Number
WO 2018/057604 A1

(51) International Patent Classification:
G06F 15/16 (2006.01) *H04L 9/32* (2006.01)
G06F 17/30 (2006.01) *H04L 29/06* (2006.01)
G06Q 20/32 (2012.01) *H04L 29/08* (2006.01)
G06Q 20/40 (2012.01) *H04W 12/06* (2009.01)
G06Q 30/02 (2012.01)

(21) International Application Number:
PCT/US2017/052482

(22) International Filing Date:
20 September 2017 (20.09.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/397,514 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 Circle, Bella Vista, AR 72714 (US). **CORSON, Gerald, Duane, III.**; 1108 North 37th Street, Rogers, AR 72756 (US). **WATTS, Charles, Alan**; 104 Blair Circle, Pea Ridge, AR 72751 (US).

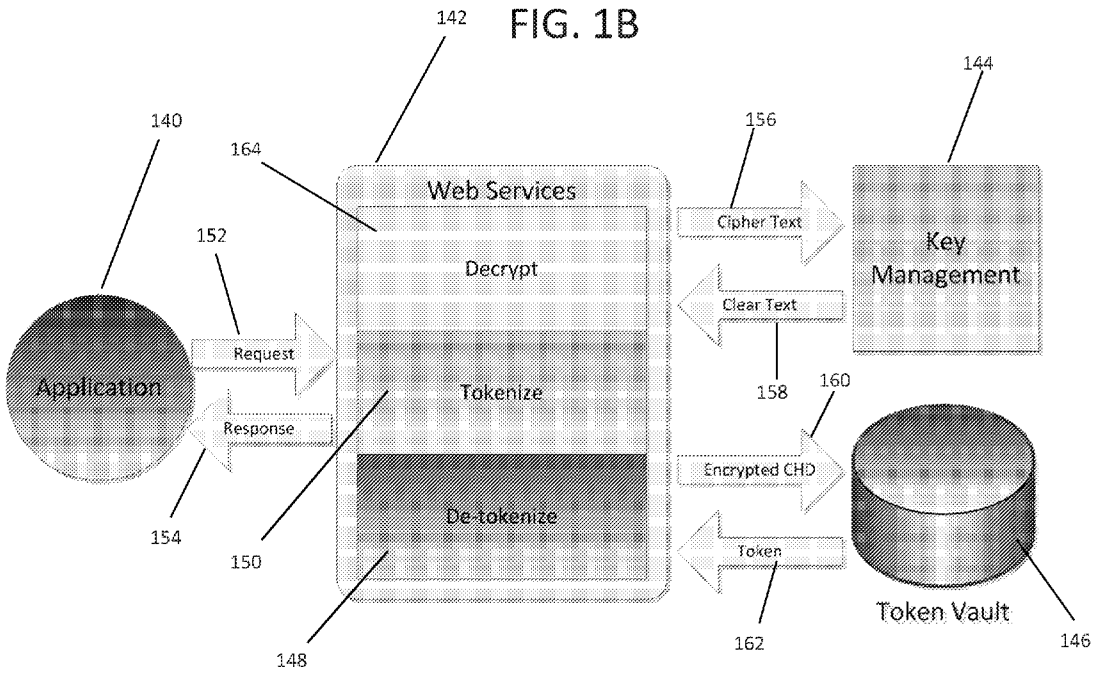
(74) Agent: **BURNS, David, R.** et al.; McCarter & English, LLP, 265 Franklin Street, Boston, MA 02110 (US).

(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, 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,

(54) Title: SYSTEM AND METHODS FOR POINT TO POINT ENCRYPTION AND TOKENIZATION USING A MOBILE DEVICE

FIG. 1B



(57) Abstract: A system and method for providing point to point encryption and tokenization using a mobile application in communication with a database. The first system is configured to receive encrypted data for transmission to a second system, to receive the response accompanied by a token representing the data, completing the transaction.

[Continued on next page]

WO 2018/057604 A1

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 USING A MOBILE DEVICE

CROSS-REFERENCE TO RELATED PATENT APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application No. 62/397,514 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 using a mobile device includes an application configured to execute on a user's mobile device and to encrypt data associated with a user. The system also includes a first computing system in communication with the mobile device and a database in communication with the first computing system. The first computing system is configured to receive encrypted data from the mobile device and to transmit the encrypted data to a second computing system hosting a Payment Card Industry Data Security Standard (PCI DSS)-compliant environment as part of a request to process the encrypted data. The first computing system is further configured to receive a response from the second computing system indicating that the processing has occurred accompanied by a token representing the data, to complete a transaction based on the response, and to transmit the token representing the data to a database for storage.

[0004] In another embodiment, a method for point to point encryption and tokenization using a mobile device includes receiving encrypted data associated with a user from an application executing on the mobile device at a first computing system, , , transmitting the encrypted data as part of a request to process the encrypted data from the first computing system to a second computing system hosting a Payment Card Industry Data Security Standard (PCI DSS)-compliant environment . The method further includes receiving a response to the request from the second computing system at the first computing system indicating that the processing has occurred. The response is accompanied by a token representing the data. The method further includes completing, via the first computing system, a transaction based on

the response, and transmitting the token representing the data from the first computing system to a database for storage.

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;

[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;

[0012] FIG. 6 is a flowchart illustrating an exemplary process performed in a point to point encryption and tokenization system when a mobile device is in communication with the first computing system time according to an exemplary embodiment; and

[0013] FIG. 7 is a flowchart illustrating an exemplary process performed in point to point encryption and tokenization in a hosted machine payment card industry (PCI) environment implementing a data security standard according to an exemplary embodiment.

DETAILED DESCRIPTION

[0014] 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.

[0015] 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 a 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.

[0016] 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 most cases of asymmetric encryption one key is a public key that may be widely distributed and the second key is a private key that is kept secret. 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 (and public access to both keys is restricted). 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.

[0017] 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.

[0018] 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.

[0019] 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.

[0020] 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.

[0021] 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.

[0022] 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.

[0023] 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. 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.

[0024] 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.

[0025] 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**). 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.

[0026] 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.

[0027] 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=.

[0028] 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.

[0029] 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.

[0030] 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.

[0031] 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.

[0032] 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.

[0033] 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.

[0034] 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.

[0035] **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**).

[0036] 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.

[0037] 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.

[0038] **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.

[0039] 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.

[0040] As discussed above, in one embodiment, instead of a user's sensitive data being encrypted by a PED, the data may instead be encrypted by a user's mobile device executing an application in communication with the first computing system. **FIG. 6** is a flowchart illustrating an exemplary process performed in a point to point encryption and tokenization system when a mobile device is in communication with the first computing system according to an exemplary embodiment. In operation 600, the first computing system (e.g. first computing system 134 and 200 as shown in **FIGS. 1A and 2**) receives encrypted data associated with a user from an application executing on a mobile device. In some embodiments, a communication pathway can be automatically established between the

mobile device and the first computing system in response to executing the application on the mobile device. For example, the encrypted data can be received by the first computing system using a proximity-based wireless communication protocol such as Blueooth™ and/or Near Field Communication. The data can be encrypted using asymmetric encryption and a public/private key pair. The encrypted data can be sensitive data such as CHD. The CHD can be credit or charge card account information associated with a user. In operation 602, the first computing system can transmit the encrypted data from the first computing system to a second computing system (e.g. second computing system 106 and 250 as shown in **FIGS. 1A and 2**) hosting a Payment Card Industry Data Security Standard (PCI DSS)-compliant environment as part of a request to process the encrypted data. The PCI DSS is a proprietary information security standard for organizations that handle financial credit cards. A PCI DSS environment aims to ensure sensitive data such as CHD is handled securely. In operation 604, the first computing system can receive a response to the request from the second computing system, indicating that the processing has occurred, the response may be accompanied by a token representing the data. For example, the response may indicate that a proposed transaction has been authorized or declined based on a user's availability of funds as inspected using the CHD. In operation 606, the first computing system can complete a transaction based on the response. For example, the first computing system may complete a sale. In operation 608, the first computing system can transmit the token representing the data to a database for storage instead of storing the originally received encrypted data. For example, the first computing system may store the token in a transaction log. In one embodiment, the first computing system may query the mobile device user for permission to store the user's data before storing the token.

[0041] The stored token may be subsequently used by the first computing system in a later occurring transaction. For example, in one embodiment, a user interacting with the first computing system through the application executing on their mobile phone may express a desire to complete a second transaction using the data previously provided by the application to the first computing system (i.e. the previously provided encrypted data). The first computing system may retrieve the stored token from the transaction log or other location and forward the token as part of a second request to the second computing system (operation 610). The token may be used by the second computing system to retrieve the earlier-provided and stored CHD and, following processing by the authentication module, a response

to the processing of the second request may be received by the first computing system from the second computing system (operation 612).

[0042] As discussed above, in one embodiment, the point to point encryption and tokenization system is hosted on a machine PCI environment implementing a data security standard. **FIG. 7** is a flowchart illustrating an exemplary process performed in point to point encryption and tokenization in a hosted machine payment card industry (PCI) environment implementing a data security standard according to an exemplary embodiment. In operation 700, the hosted machine PCI environment can receive encrypted card holder data (CHD) from an external system with a computing system operatively coupled to a database in the hosted machine PCI environment, . For example, the external system can be the first computing system (e.g. first computing system 134 and 200 as shown in **FIGS. 1A and 2**) and the computing system in the hosted machine PCI environment can be the second computing system (e.g. second computing system 106 and 250 as shown in **FIGS. 1A and 2**). The external system can receive the external data from a (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**). The computing system in the hosted machine PCI environment can include processing zones. Each processing zone can hold one or more processing modules. The processing modules can include a decryption module (e.g. decryption module 120 and 164 as shown in **FIG. 1A-B**), a tokenization module (e.g. tokenization module 122 and 150 as shown in **FIG. 1A-B**) and an authorization module (e.g. authorization module 104 as shown in **FIG. 1A**). The data transfers between the processing zones can be monitored and restricted according to pre-defined policies using a number of different security techniques as discussed above. The processing modules can further include a web services module (e.g. web-services module 126 and 142 as shown in **FIG. 1A-B**) implemented as middleware in the computing system in the hosted machine PCI environment. The web services module can use a representational state transfer (REST) architecture. The computing system can include a certificate authority server (e.g. certificate authority server 112 as shown in **FIG. 1A**) which can host a key management system (e.g. public key server 110 or key management module 144 as shown in **FIG. 1A-B**) configured to issue public keys and store security certificates.

[0043] In operation 702, the decryption module can decrypt the encrypted CHD. The decryption module can be a Hardware Security Module (HSM). In operation 704, the tokenization module can generate a token representing the decrypted CHD. In operation 706,

the authorization module can process the decrypted CHD based on the request from the external computing system. In operation 708, a confirmation of the processing can be transmitted to the external computing system. For example, the confirmation may indicate that a proposed transaction has been authorized or declined based on a user's availability of funds as inspected via the authorization module using the CHD. In operation 710, the computing system in the PCI environment can store the token representing the decrypted CHD and the decrypted CHD in the database, such as a token vault (e.g. token vault 245 as shown in **FIG. 2**).

[0044] The stored token may be subsequently used by the external computing system in a later occurring transaction. For example, in one embodiment, a user interacting with the external computing system may wish to perform a second transaction using the data previously provided by the application to the external computing system (i.e. the previously provided encrypted data). The external computing system may retrieve and forward the token as part of a second request to the computing system in the hosted machine PCI environment. The token may be used by the computing system in the PCI environment to retrieve the earlier-provided CHD from the database and the authentication module can process the transaction using the CHD (operation 712). In operation 714, the a response to the processing of the second request within the PCI environment may be received by the external computing system.

[0045] 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 multiple 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 multiple 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.

[0046] 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 using a mobile device, the system comprising:

an application configured to execute on a user's mobile device and to encrypt data associated with a user;

a first computing system in communication with the mobile device ; and

a database in communication with the first computing system,

wherein the first computing system is configured to:

receive encrypted data from the mobile device,

transmit the encrypted data to a second computing system hosting a Payment Card Industry Data Security Standard (PCI DSS)-compliant environment as part of a request to process the encrypted data,

receive, a response from the second computing system indicating that the processing has occurred accompanied by a token representing the data,

complete a transaction based on the response, and

transmit the token representing the data to a database for storage.

2. The system of claim 1, wherein the mobile device is configured to:

automatically connect to the first computing system in response to executing the application.

3. The system of claim 1, wherein the first computing system is further configured to:

receive the encrypted data using a proximity-based wireless communication protocol.

4. The system of claim 3, wherein the proximity-based wireless communication protocol is one of Blueooth™ and Near Field Communication.

5. The system of claim 1 wherein the data associated with the user is card holder data associated with a credit card or charge card of the user.

6. The system of claim 1, wherein the first computing system is further configured to:

receive an authorization from the second computing system and in response store a token representing the data in a transaction log.

7. The system of claim 1, wherein the first computing system and the second computing system are located in different geographic locations.

8. The system of claim 1, wherein the data is encrypted using asymmetric encryption.

9. The system of claim 1, wherein the first computing system is further configured to:

receive a request from the mobile device requiring a subsequent use of the data;

retrieve the token from the database in response to the mobile device request;

transmit the token and a new request for further processing of the data to the second computing system; and

receive a response to the new request regarding the further processing from the second computing system,

wherein the second computing system uses the token representing the data to retrieve the data and perform the further processing.

10. The system of claim 1, wherein the first computing system is further configured to:

receive an authorization from the second computing system in response to the second request and to store a token representing the data in a transaction log.

11. A point to point encryption and tokenization method using a mobile device, the method comprising:

receiving at a first computing system, from an application executing on a mobile device associated with a user, encrypted data associated with the user,

transmitting the encrypted data from the first computing system to a second computing system hosting a Payment Card Industry Data Security Standard (PCI DSS)-compliant environment as part of a request to process the encrypted data,

receiving a response to the request from the second computing system at the first computing system indicating that the processing has occurred, the response accompanied by a token representing the data,

completing, via the first computing system, a transaction based on the response, and

transmitting the token representing the data from the first computing system to a database for storage.

12. The method of claim 11, further comprising:

establishing automatically a communication pathway between the mobile device and the first computing system in response to the mobile device beginning execution of the application.

13. The method of claim 11, further comprising:

receiving with the first computing system the encrypted data using a proximity-based wireless communication protocol.

14. The method of claim 13, wherein the proximity-based wireless communication protocol is one of Blueooth™ and Near Field Communication.

15. The method of claim 11, wherein the data associated with the user is card holder data associated with a credit card or charge card of the user.

16. The method of claim 11, further comprising:

receiving with the first computing system an authorization from the second computing system and in response storing a token representing the data in a transaction log.

17. The method of claim 11, wherein the first computing system and the second computing system are located in different geographic locations.

18. The method of claim 11, wherein the data is encrypted using asymmetric encryption.

19. The method of claim 11, further comprising:

receiving a request from the mobile device requiring a subsequent use of the data;

retrieving the token from the database in response to the mobile device request;

transmitting the token and a new request for further processing of the data to the second computing system; and

receiving a response to the new request regarding the further processing from the second computing system,

wherein the second computing system uses the token representing the data to retrieve the data and perform the further processing.

20. The method of claim 11, further comprising:

receiving an authorization from the second computing system in response to the second request and to store a token representing the data in a transaction log.

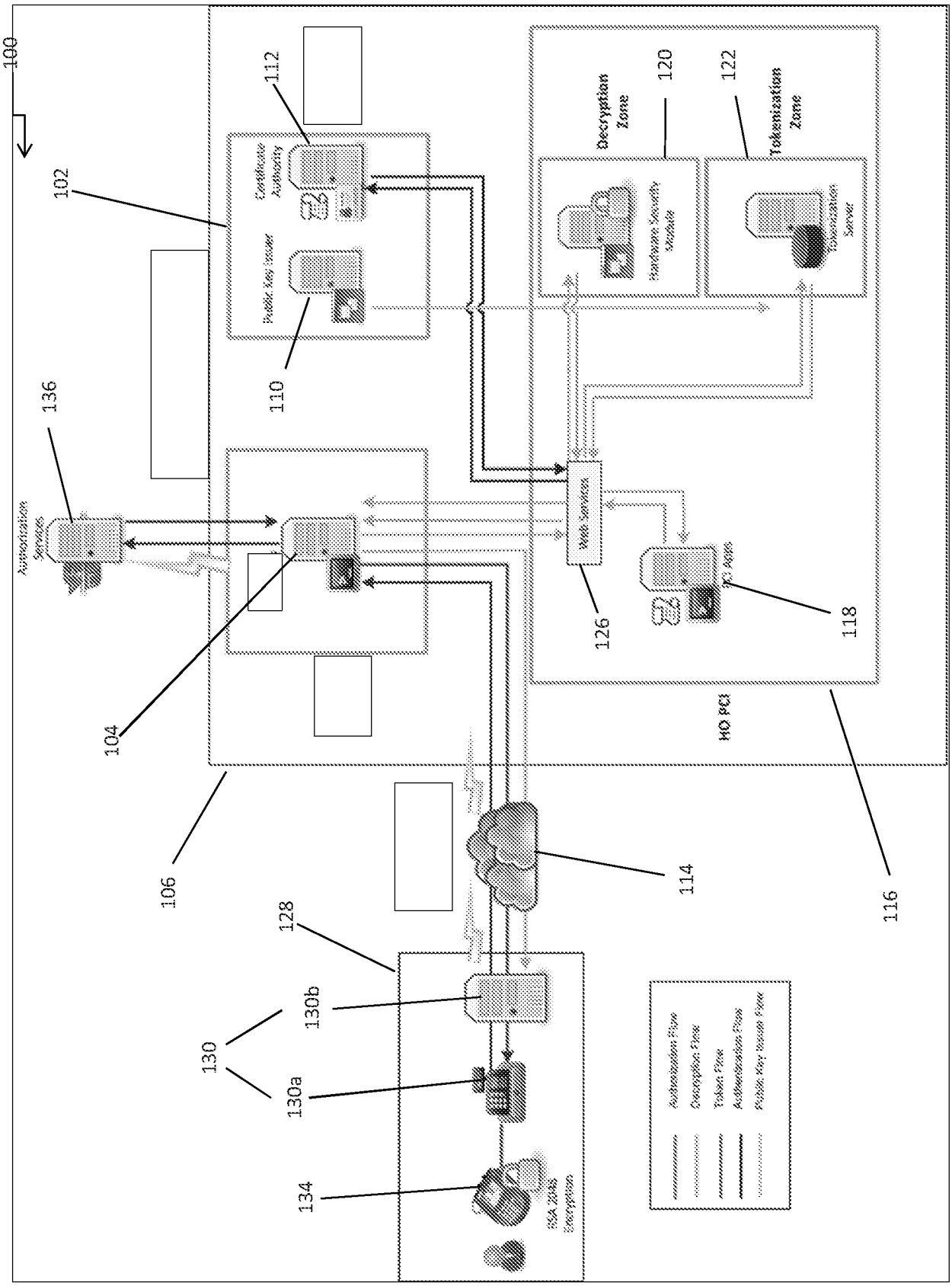

100
102
104
106
110
112
114
116
118
120
122
126
128
130
130a
130b
134
136
Decryption Zone
Tokenization Zone
Certificate Authority
Public Key Issuer
Hardware Security Module
Tokenization Server
Authentication Services
Web Services
PCI Apps
HSM Apps
Encryption
PCI
Authentication Flow
Decryption Flow
Token Flow
Authentication Flow
Public Key Issuer Flow

FIG. 1A

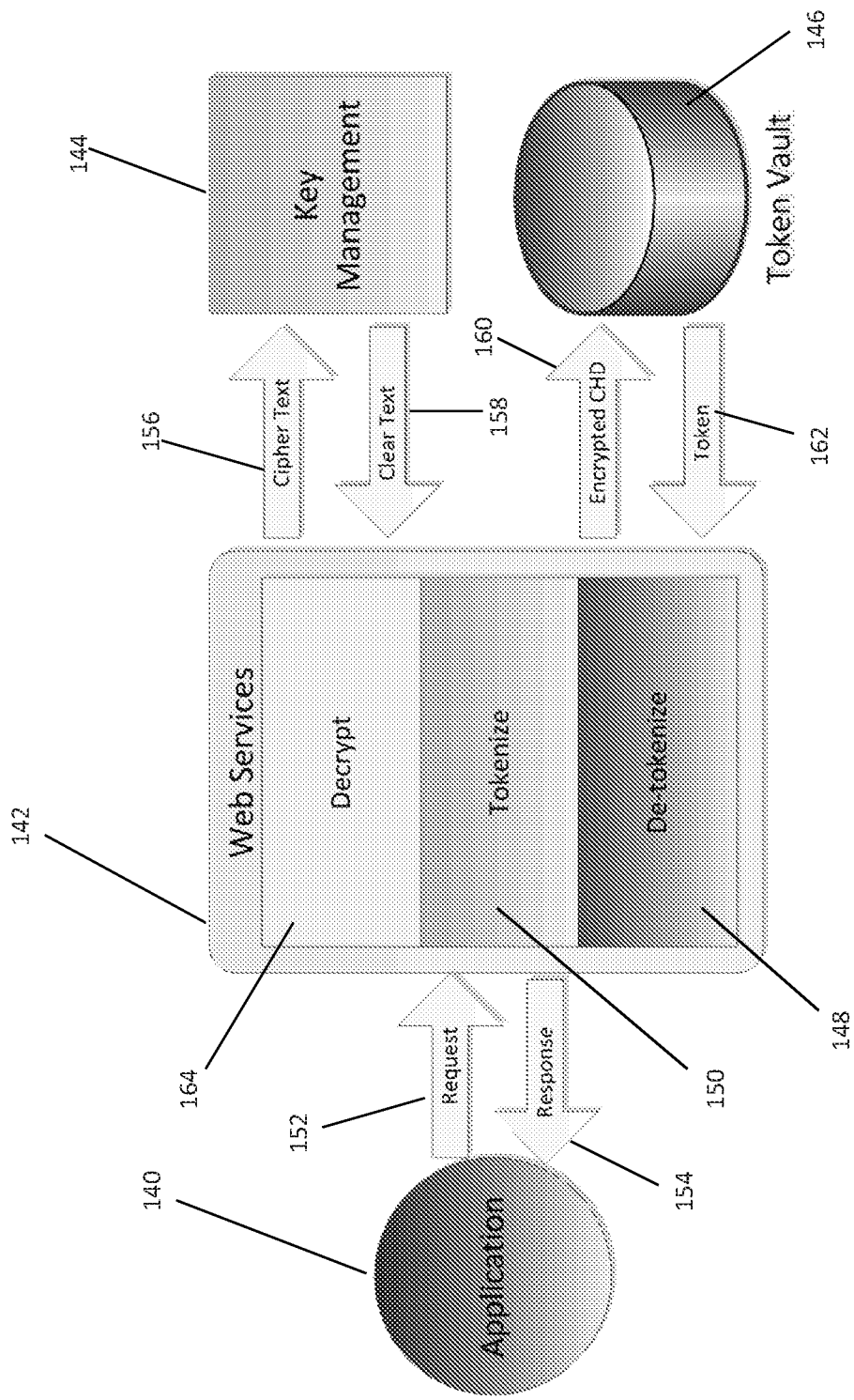

Key Management
144
Token Vault
146
160
Cipher Text
156
Clear Text
158
Encrypted CHD
Token
162
Web Services
142
Decrypt
Tokenize
De-tokenize
164
150
148
Request
Response
152
154
Application
140

FIG. 1B

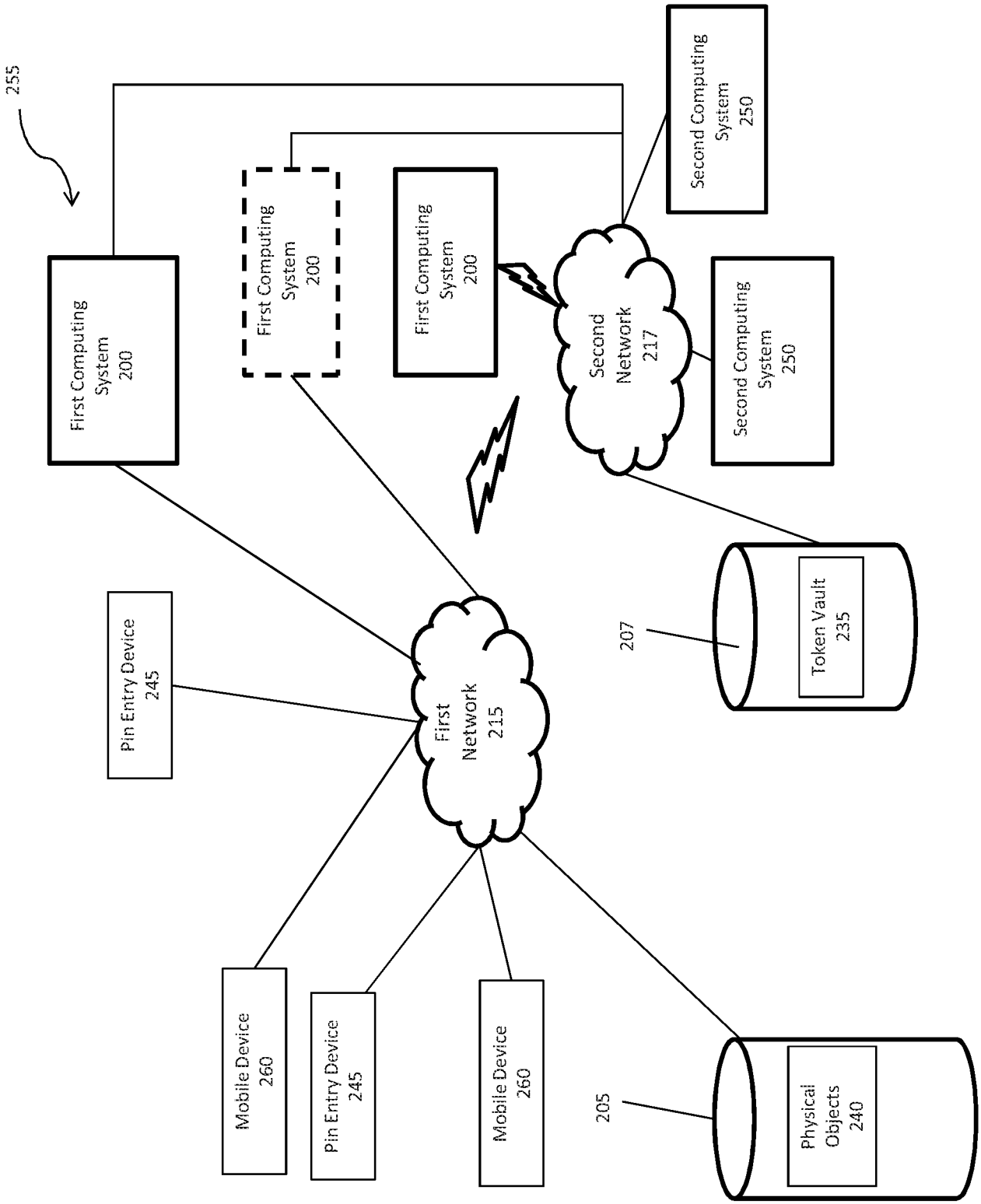

255
First Computing System 200
First Computing System 200
First Computing System 200
Second Computing System 250
Second Computing System 250
Second Network 217
Pin Entry Device 245
First Network 215
207
Token Vault 235
Mobile Device 260
Pin Entry Device 245
Mobile Device 260
205
Physical Objects 240

FIG. 2

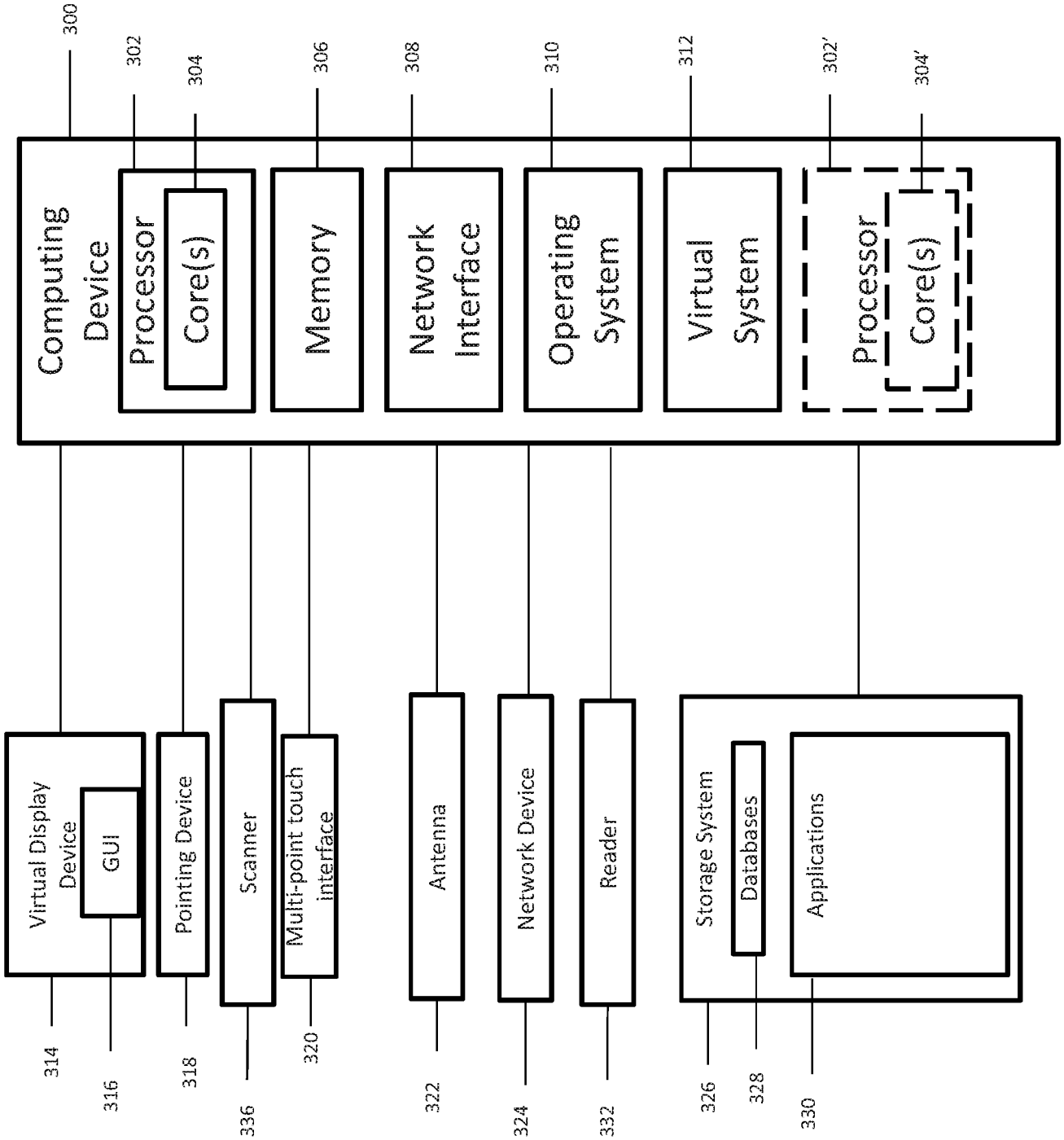

300
302
304
306
308
310
312
302'
304'
Computing Device
Processor
Core(s)
Memory
Network Interface
Operating System
Virtual System
Processor
Core(s)
Virtual Display Device
GUI
Pointing Device
Scanner
Multi-point touch interface
Antenna
Network Device
Reader
Storage System
Databases
Applications
314
316
318
336
320
322
324
332
326
328
330

FIG. 3

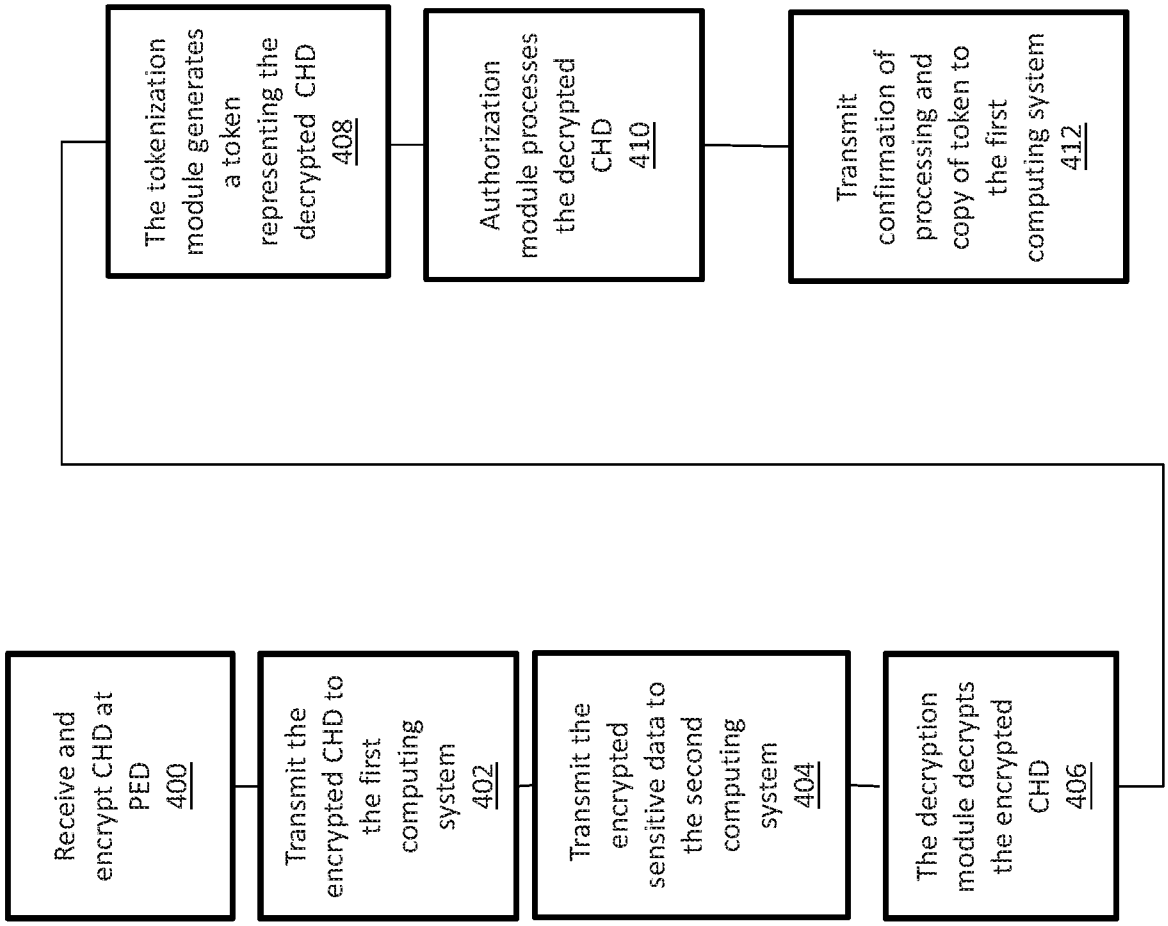

Receive and encrypt CHD at PED 400
Transmit the encrypted CHD to the first computing system 402
Transmit the encrypted sensitive data to the second computing system 404
The decryption module decrypts the encrypted CHD 406
The tokenization module generates a token representing the decrypted CHD 408
Authorization module processes the decrypted CHD 410
Transmit confirmation of processing and copy of token to the first computing system 412

FIG. 4

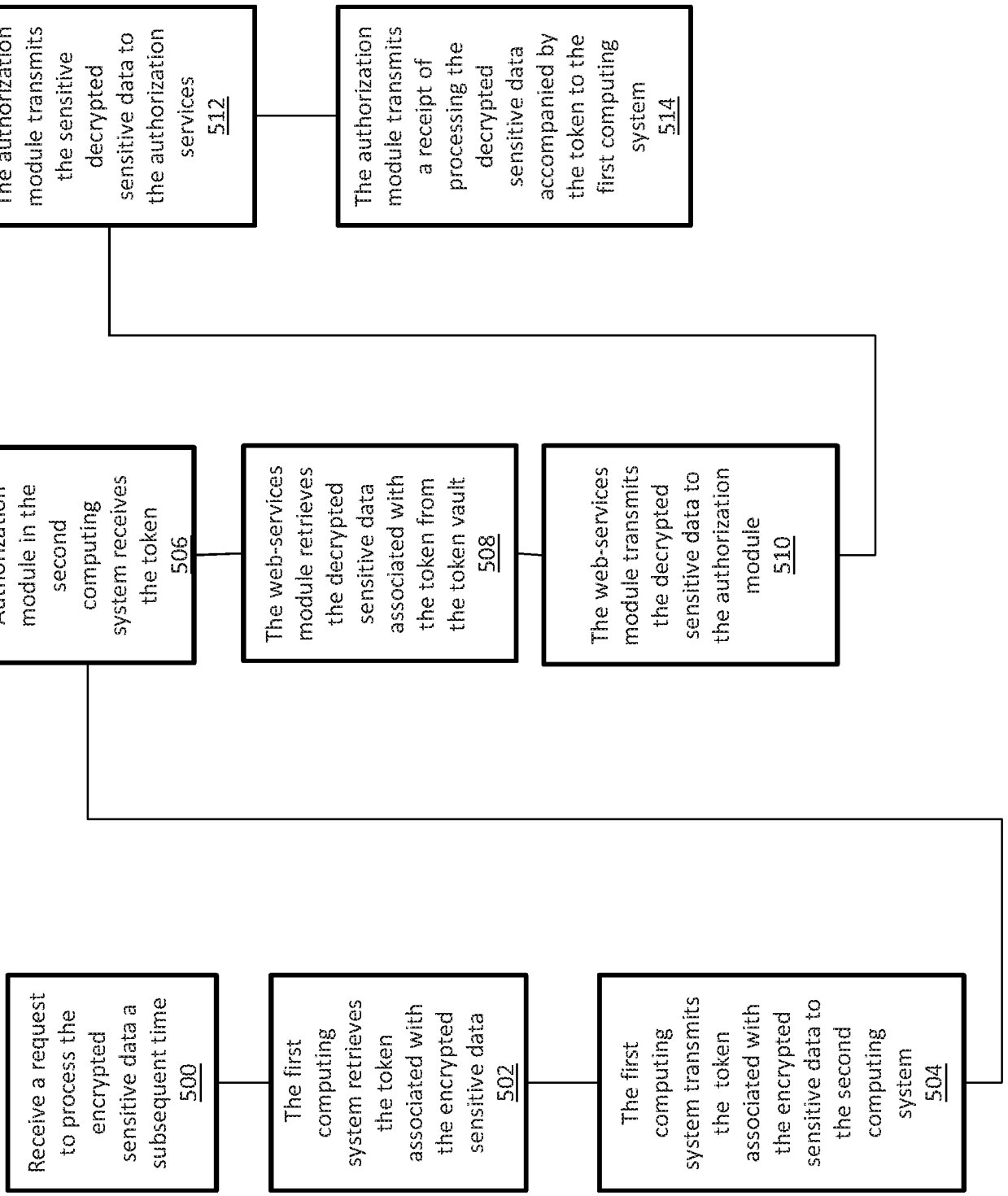

Receive a request to process the encrypted sensitive data a subsequent time 500
The first computing system retrieves the token associated with the encrypted sensitive data 502
The first computing system transmits the token associated with the encrypted sensitive data to the second computing system 504
Authorization module in the second computing system receives the token 506
The web-services module retrieves the decrypted sensitive data associated with the token from the token vault 508
The web-services module transmits the decrypted sensitive data to the authorization module 510
The authorization module transmits the sensitive decrypted sensitive data to the authorization services 512
The authorization module transmits a receipt of processing the decrypted sensitive data accompanied by the token to the first computing system 514

FIG. 5

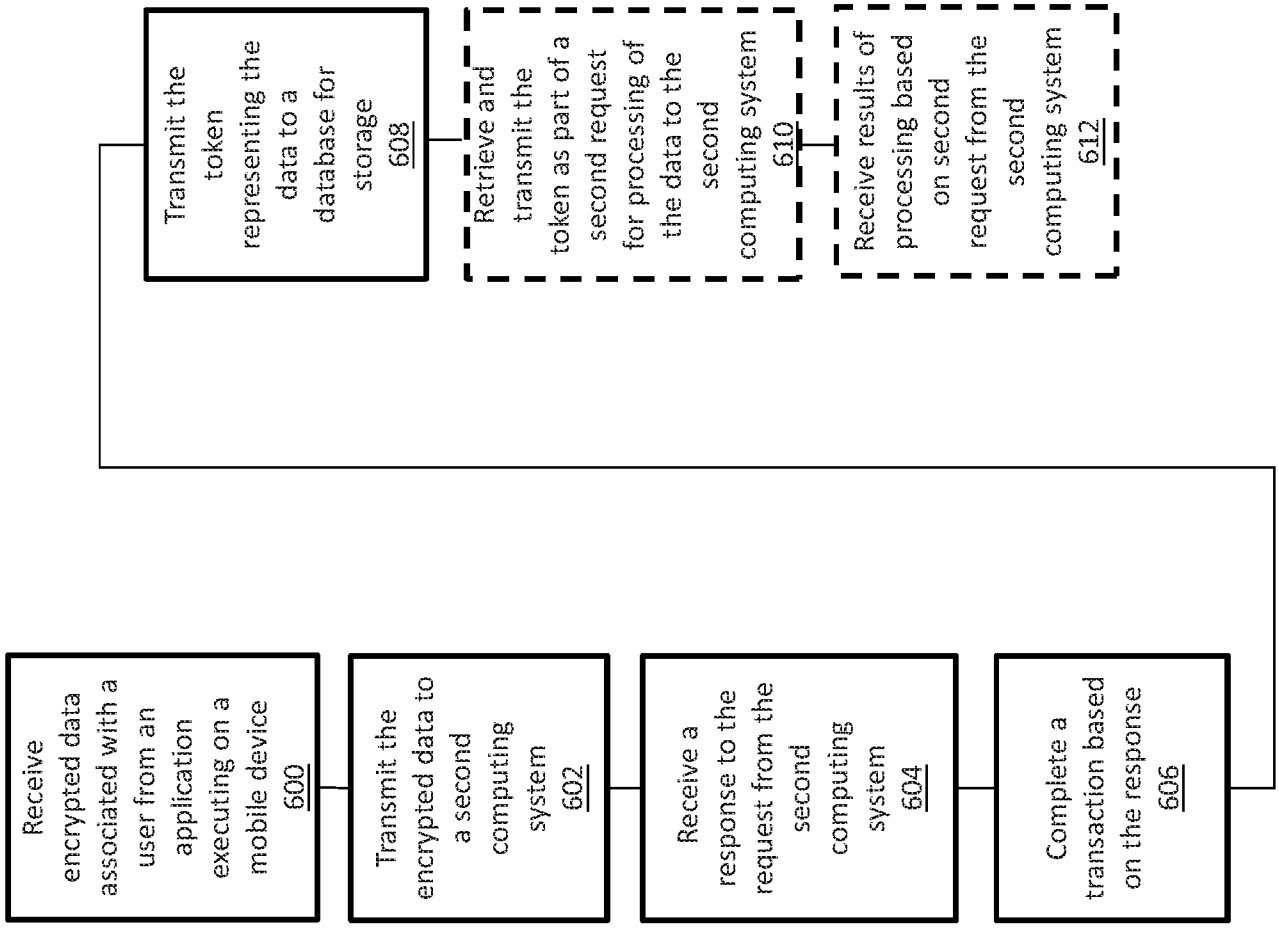

Receive encrypted data associated with a user from an application executing on a mobile device 600
Transmit the encrypted data to a second computing system 602
Receive a response to the request from the second computing system 604
Complete a transaction based on the response 606
Transmit the token representing the data to a database for storage 608
Retrieve and transmit the token as part of a second request for processing of the data to the second computing system 610
Receive results of processing based on second request from the second computing system 612

FIG. 6

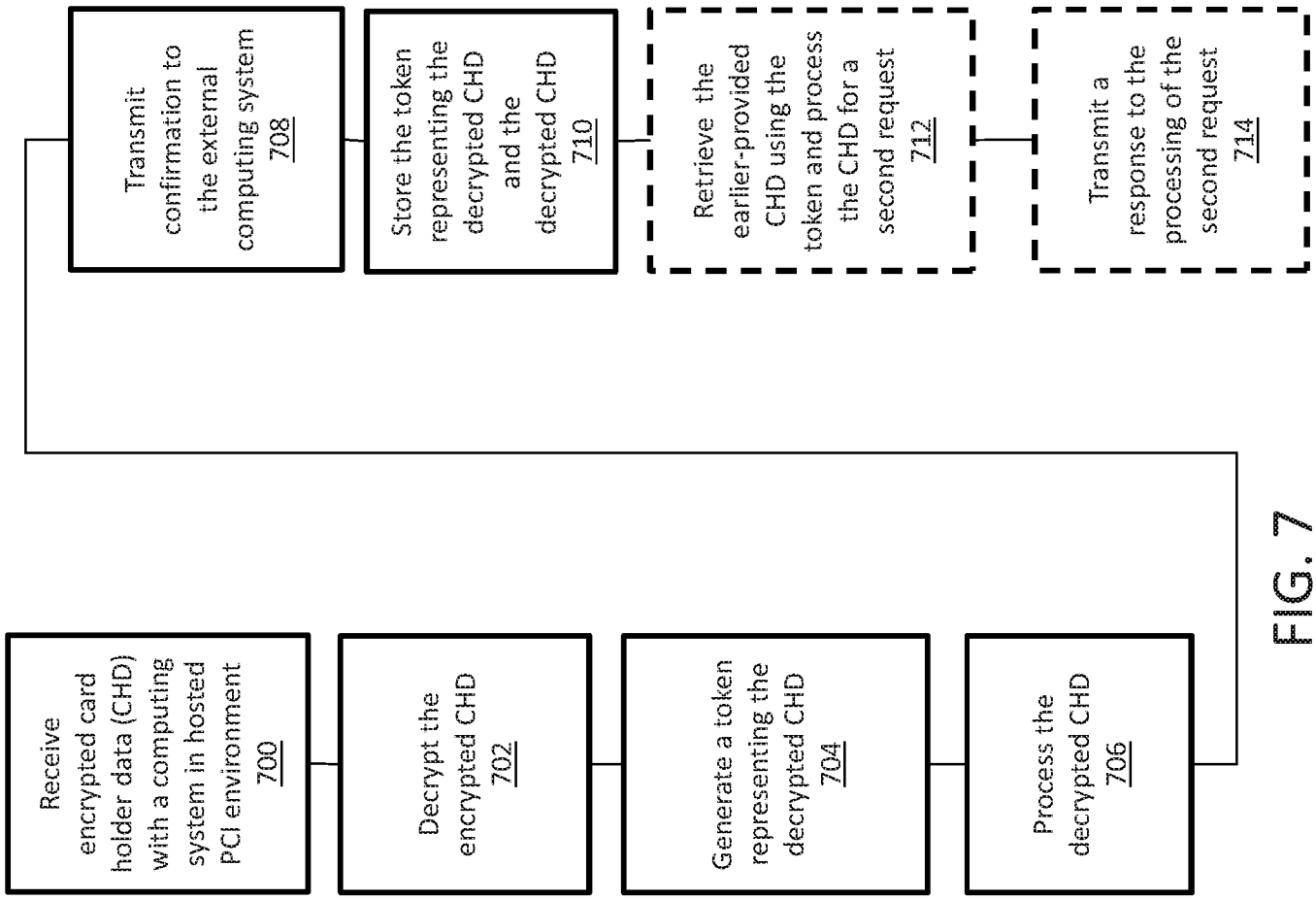

Receive encrypted card holder data (CHD) with a computing system in hosted PCI environment 700
Decrypt the encrypted CHD 702
Generate a token representing the decrypted CHD 704
Process the decrypted CHD 706
Transmit confirmation to the external computing system 708
Store the token representing the decrypted CHD and the decrypted CHD 710
Retrieve the earlier-provided CHD using the token and process the CHD for a second request 712
Transmit a response to the processing of the second request 714

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/52482

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 15/16, 17/30; G06Q 20/32, 20/40, 30/02; H04L 9/32, 29/06, 29/08; H04W 12/06 (2017.01)

CPC - G06F 15/16, 17/30, 21/00; G06Q 20/32, 20/322, 20/382, 20/40, 30/02; H04L 63/0428, 63/08, 63/0823, 63/083; H04W 12/02, 12/04, 12/06, 12/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2014/0108172 A1 (WEBER, L et al.) 17 April 2014; abstract; figures 1-3, 10; [0013], [0016], [0032]-[0034], [0037]-[0045], [0056]-[0059], [0064], [0071]-[0077], [0131]-[0135].	1-6, 8-16, 18-20 ---------- 7, 17
Y	US 2011/0258123 A1 (DAWKINS, J et al.) 20 October 2011; abstract; figure 1; paragraphs [0035], [0066].	7, 17
A	US 2014/0366151 A1 (MCGUIRE, K et al.) 11 December 2014; entire document.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 November 2017 (09.11.2017)	27 NOV 2017
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)