US010829088B2

(12) **United States Patent**
Jarvis et al.

(10) **Patent No.: US 10,829,088 B2**
(45) **Date of Patent: Nov. 10, 2020**

(54) **IDENTITY MANAGEMENT FOR IMPLEMENTING VEHICLE ACCESS AND OPERATION MANAGEMENT**

(71) Applicant: **SENSORMATIC ELECTRONICS, LLC**, Boca Raton, FL (US)

(72) Inventors: **Graeme Jarvis**, Marblehead, MA (US); **Terezinha Rumble**, Jensen Beach, FL (US); **George C. Grammer**, West Palm Beach, FL (US); **Michael Lamarca**, Parker, CO (US)

(73) Assignee: **SENSORMATIC ELECTRONICS, LLC**, Boca Raton, FL (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **15/911,512**

(22) Filed: **Mar. 5, 2018**

(65) **Prior Publication Data**

US 2019/0092279 A1 Mar. 28, 2019

Related U.S. Application Data

(60) Provisional application No. 62/561,743, filed on Sep. 22, 2017.

(51) **Int. Cl.**
B60R 25/24 (2013.01)
G06Q 20/00 (2012.01)
(Continued)

(52) **U.S. Cl.**
CPC ***B60R 25/24*** (2013.01); ***G06F 21/00*** (2013.01); ***G06F 21/31*** (2013.01); ***G06Q 10/06*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC B60R 25/24; B60R 2325/108; G07F 17/0057; G06Q 20/3224; H04L 9/3239
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,743,349 A * 4/1998 Steinberg B60K 28/063 180/272
6,259,405 B1 7/2001 Stewart et al.
(Continued)

FOREIGN PATENT DOCUMENTS

WO WO-2018/048640 3/2018
WO WO-2018/048651 3/2018
(Continued)

OTHER PUBLICATIONS

Office Action for U.S. Appl. No. 15/911,613, dated Nov. 13, 2018, 39 pages.

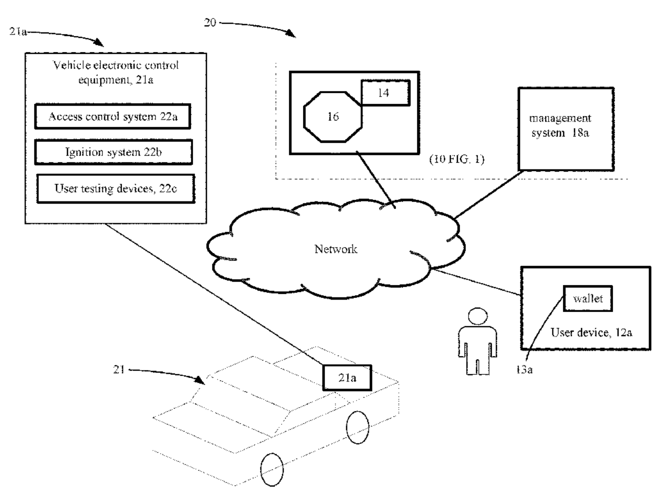
(Continued)

Primary Examiner — Vernal U Brown
(74) *Attorney, Agent, or Firm* — Foley & Lardner LLP

(57) **ABSTRACT**

Described are techniques for monitoring use of a shared resource, such as physical resource, for example, a motor vehicle. The techniques include receiving an electronic representation of a user's identity, by a vehicle access application executable in a computing system in the vehicle, sending by the computing system to an identity and access management system the received electronic representation of the user's identity, receiving by the computing system from the identity and access management system credentials that validate the electronic representation of the user's identity, and enabling by the computing system starting of the vehicle when the computing system receives the credentials that validated the user's identity.

20 Claims, 20 Drawing Sheets



(51) **Int. Cl.**

G07F 17/00	(2006.01)
G07C 1/00	(2006.01)
G06F 21/00	(2013.01)
G06Q 20/38	(2012.01)
G06Q 20/32	(2012.01)
H04L 9/32	(2006.01)
G06Q 10/06	(2012.01)
G07C 9/00	(2020.01)
G06F 21/31	(2013.01)

(52) **U.S. Cl.**
CPC ***G06Q 20/00*** (2013.01); ***G06Q 20/3223*** (2013.01); ***G06Q 20/3224*** (2013.01); ***G06Q 20/3274*** (2013.01); ***G06Q 20/385*** (2013.01); ***G06Q 20/3823*** (2013.01); ***G07C 1/00*** (2013.01); ***G07C 9/00571*** (2013.01); ***G07F 17/0057*** (2013.01); ***H04L 9/3239*** (2013.01); ***H04L 9/3247*** (2013.01); ***H04L 9/3297*** (2013.01); *B60R 2325/108* (2013.01); *G06Q 2220/00* (2013.01); *H04L 2209/38* (2013.01); *H04L 2209/56* (2013.01)

(58) **Field of Classification Search**
USPC 340/5.6
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,748,792	B1 *	6/2004	Freund	B60K 28/063 180/272
7,043,443	B1	5/2006	Firestone	
8,344,850	B2	1/2013	Girard et al.	
9,589,405	B2	3/2017	Cabouli et al.	
9,858,781	B1	1/2018	Campero et al.	
10,055,926	B2	8/2018	Campero et al.	
10,453,319	B2	10/2019	Jarvis et al.	
10,475,272	B2	11/2019	Campero et al.	
10,475,273	B2	11/2019	Campero et al.	
2006/0184456	A1 *	8/2006	de Janasz	G06Q 20/12 705/72
2008/0243561	A1	10/2008	Deygout et al.	
2009/0210308	A1	8/2009	Toomer et al.	
2011/0060480	A1	3/2011	Mottla et al.	
2011/0202393	A1	8/2011	Dewakar et al.	
2013/0317693	A1	11/2013	Jeffries et al.	
2014/0090036	A1	3/2014	Roberts	
2014/0091903	A1	4/2014	Birkel et al.	
2014/0351328	A1	11/2014	Woods et al.	
2015/0095190	A1	4/2015	Hammad et al.	
2015/0278508	A1	10/2015	Johnson	
2015/0286670	A1	10/2015	Hall et al.	
2016/0036788	A1	2/2016	Conrad et al.	
2016/0134599	A1	5/2016	Ross et al.	
2016/0180618	A1	6/2016	Ho et al.	
2016/0189528	A1	6/2016	Lee et al.	
2016/0217280	A1	7/2016	Oberheide et al.	
2017/0111175	A1	4/2017	Oberhauser et al.	
2017/0214675	A1 *	7/2017	Johnsrud	H04L 63/08
2017/0300898	A1 *	10/2017	Campero	H04L 9/3236
2018/0041860	A1 *	2/2018	England	H04B 5/0031
2018/0072416	A1 *	3/2018	Cantrell	B64C 39/024
2018/0075247	A1	3/2018	Campero et al.	
2018/0075677	A1	3/2018	Campero et al.	
2018/0077151	A1	3/2018	Campero et al.	
2018/0194323	A1 *	7/2018	Woodill, Jr.	G07C 9/00
2019/0087781	A1	3/2019	Mercury et al.	
2019/0188941	A1	6/2019	Campero et al.	

FOREIGN PATENT DOCUMENTS

WO	WO-2018/048662	3/2018
WO	WO-2018/048663	3/2018
WO	WO-2018/048691	3/2018
WO	WO-2018/048692	3/2018

OTHER PUBLICATIONS

European Search Report, EP Application No. 18196220, dated Jan. 17, 2019, 8 pages.

Melanie Swan, E-Commerce, Jan. 22, 2015, XP055406241, http://w2.blockchain-tec.net/blockchain/blockchain-by?melanie-swan.pdf, 149 pages.

European Search Report, EP Application No. 18195939.6, dated Feb. 27, 2019, 9 pages.

European Search Report, EP Application No. 18196020.4, dated Feb. 27, 2019, 8 pages.

European Search Report, EP Application No. 18195994.1, dated Feb. 27, 2019, 7 pages.

* cited by examiner

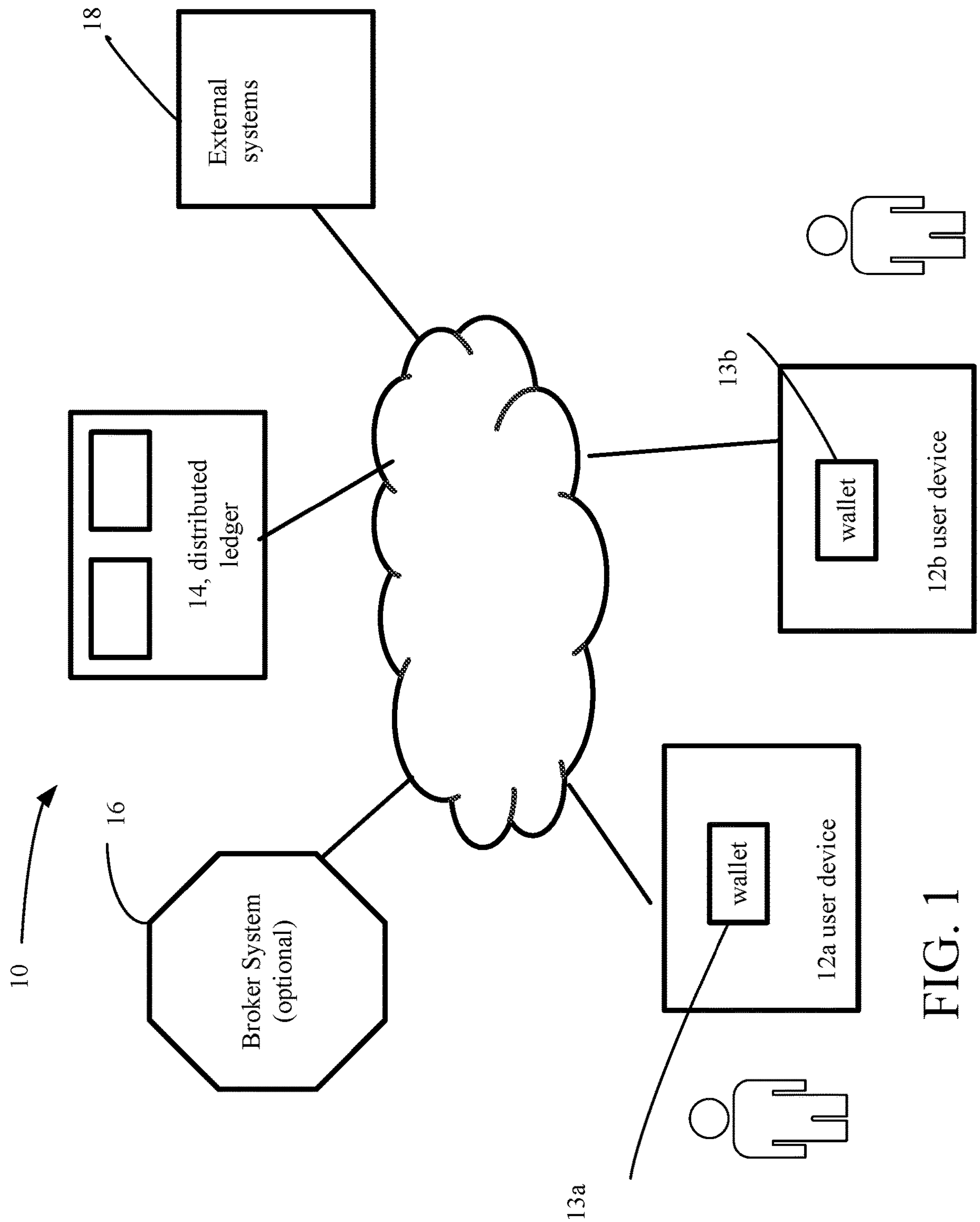
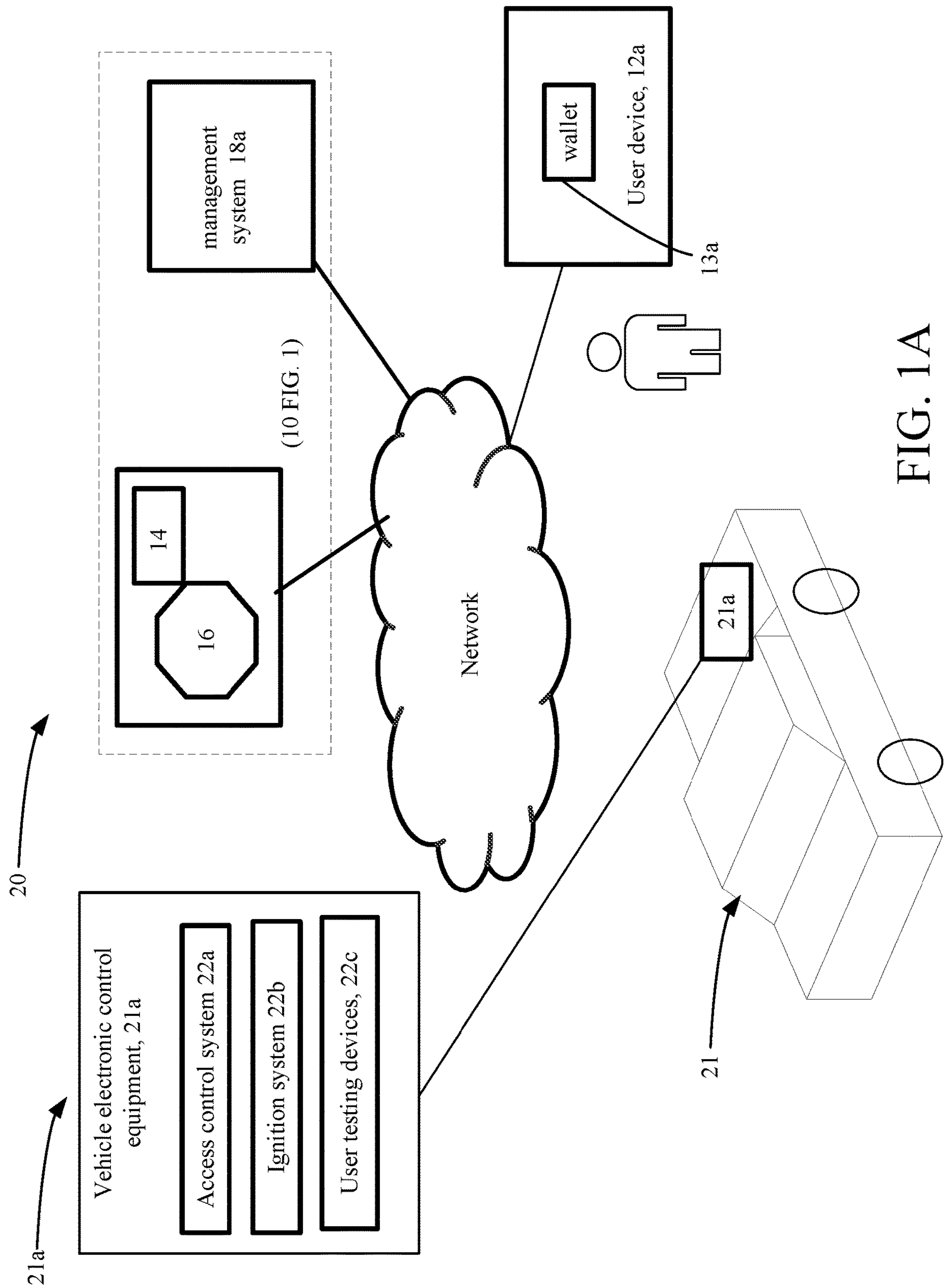

10
16
Broker System (optional)
14, distributed ledger
18
External systems
13a
wallet
12a user device
13b
wallet
12b user device

FIG. 1



management system 18a
(10 FIG. 1)
14
16
Network
wallet
User device, 12a
13a
20
21a
Vehicle electronic control equipment, 21a
Access control system 22a
Ignition system 22b
User testing devices, 22c
21a
21

FIG. 1A

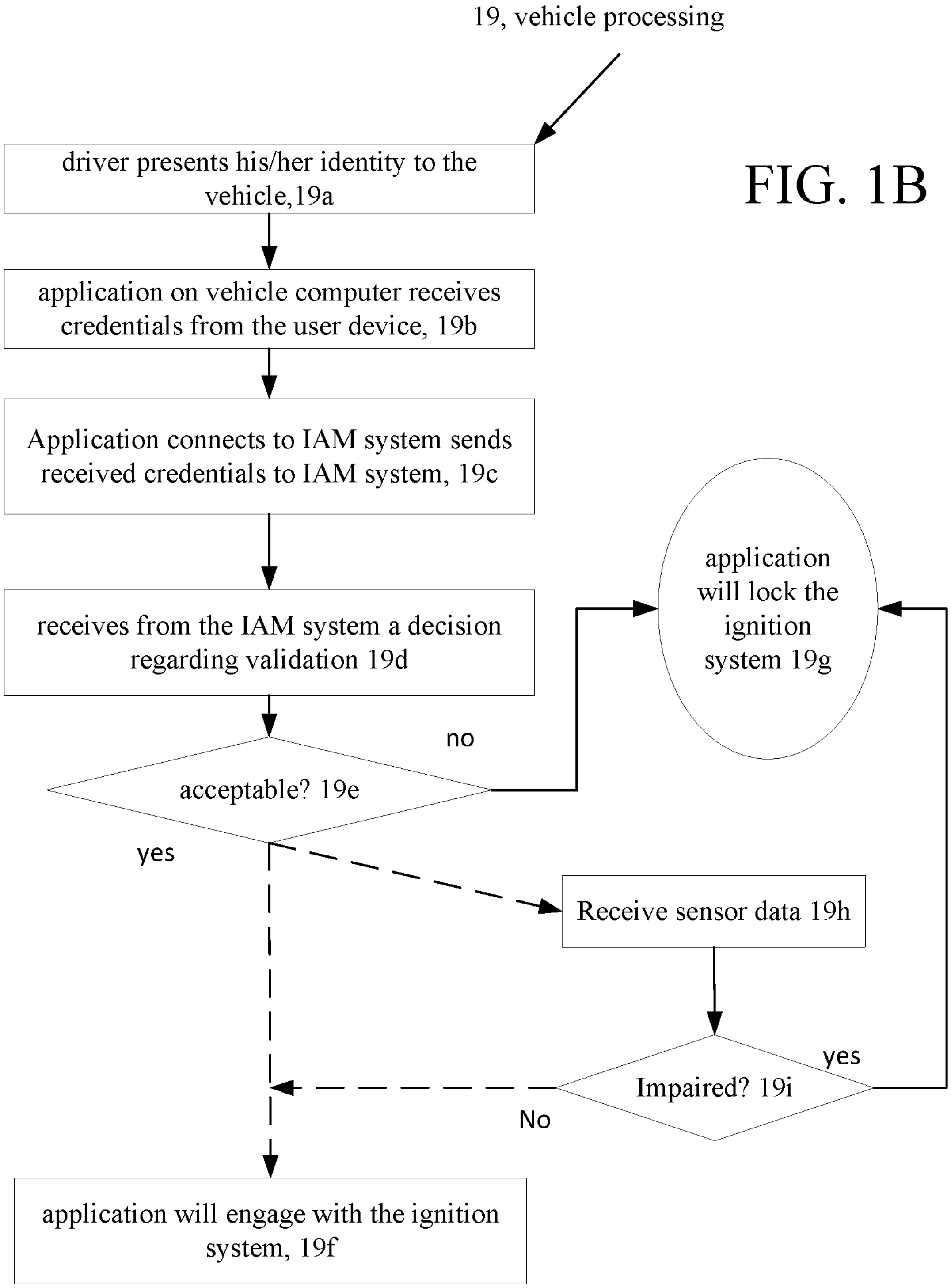

19, vehicle processing
driver presents his/her identity to the vehicle,19a
application on vehicle computer receives credentials from the user device, 19b
Application connects to IAM system sends received credentials to IAM system, 19c
receives from the IAM system a decision regarding validation 19d
acceptable? 19e
no
yes
application will lock the ignition system 19g
Receive sensor data 19h
Impaired? 19i
yes
No
application will engage with the ignition system, 19f

FIG. 1B

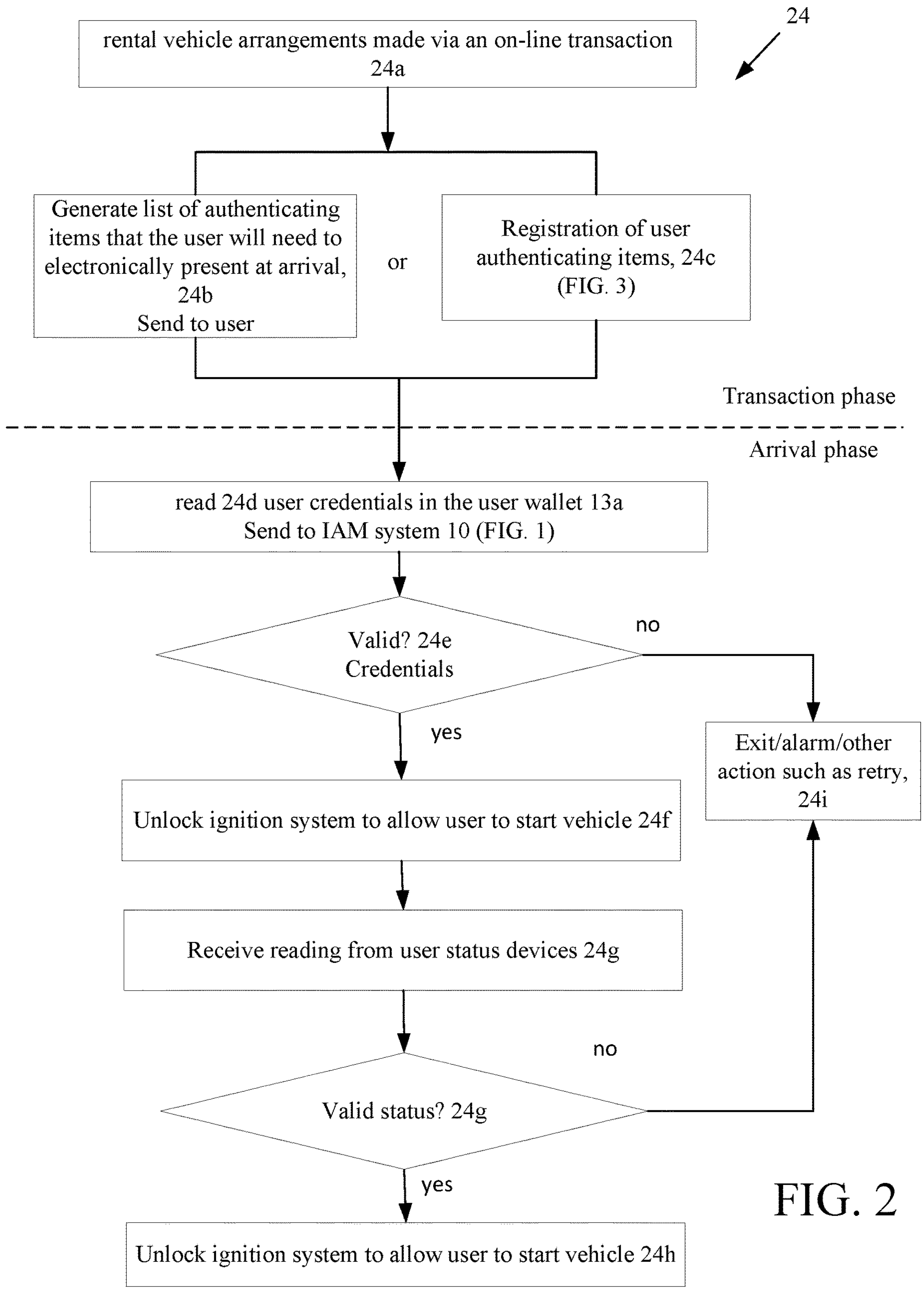

24
rental vehicle arrangements made via an on-line transaction 24a
Generate list of authenticating items that the user will need to electronically present at arrival, 24b
Send to user
or
Registration of user authenticating items, 24c (FIG. 3)
Transaction phase
Arrival phase
read 24d user credentials in the user wallet 13a
Send to IAM system 10 (FIG. 1)
Valid? 24e Credentials
no
yes
Exit/alarm/other action such as retry, 24i
Unlock ignition system to allow user to start vehicle 24f
Receive reading from user status devices 24g
no
Valid status? 24g
yes
Unlock ignition system to allow user to start vehicle 24h

FIG. 2

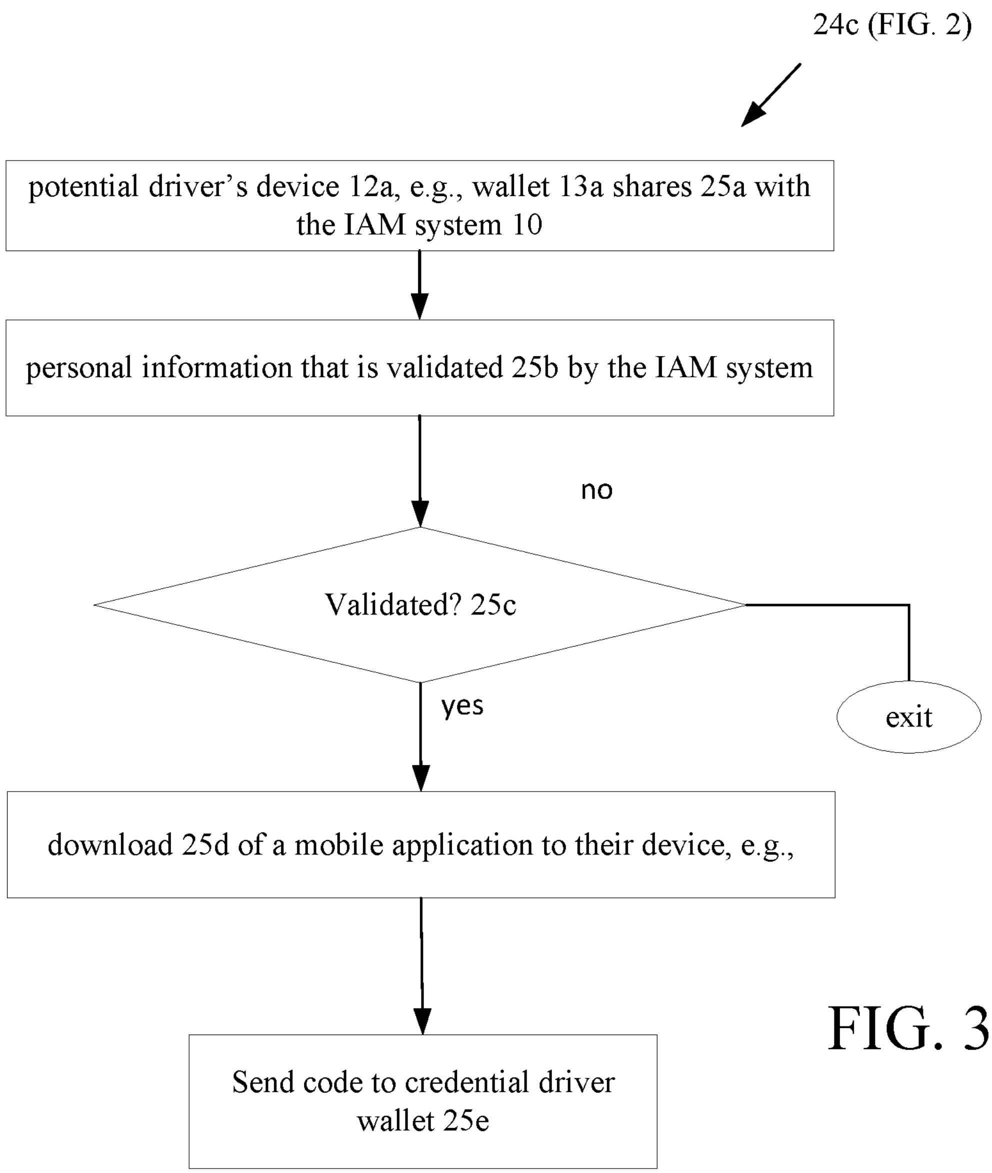
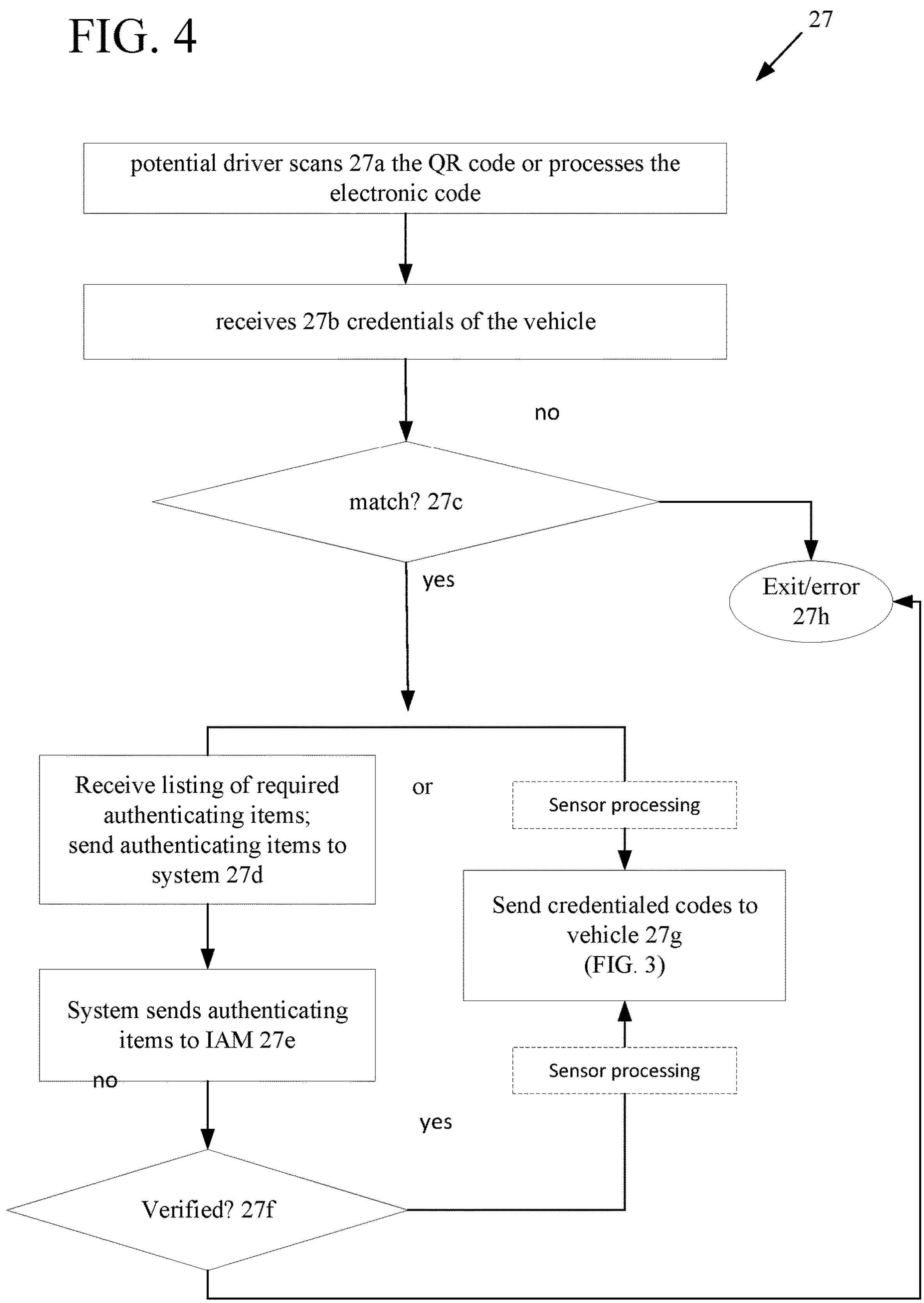

24c (FIG. 2)
potential driver's device 12a, e.g., wallet 13a shares 25a with the IAM system 10
personal information that is validated 25b by the IAM system
no
Validated? 25c
yes
exit
download 25d of a mobile application to their device, e.g.,
Send code to credential driver wallet 25e

FIG. 3

FIG. 4


27
potential driver scans 27a the QR code or processes the electronic code
receives 27b credentials of the vehicle
no
match? 27c
yes
Exit/error 27h
Receive listing of required authenticating items; send authenticating items to system 27d
or
Sensor processing
Send credentialed codes to vehicle 27g (FIG. 3)
System sends authenticating items to IAM 27e
no
Sensor processing
yes
Verified? 27f

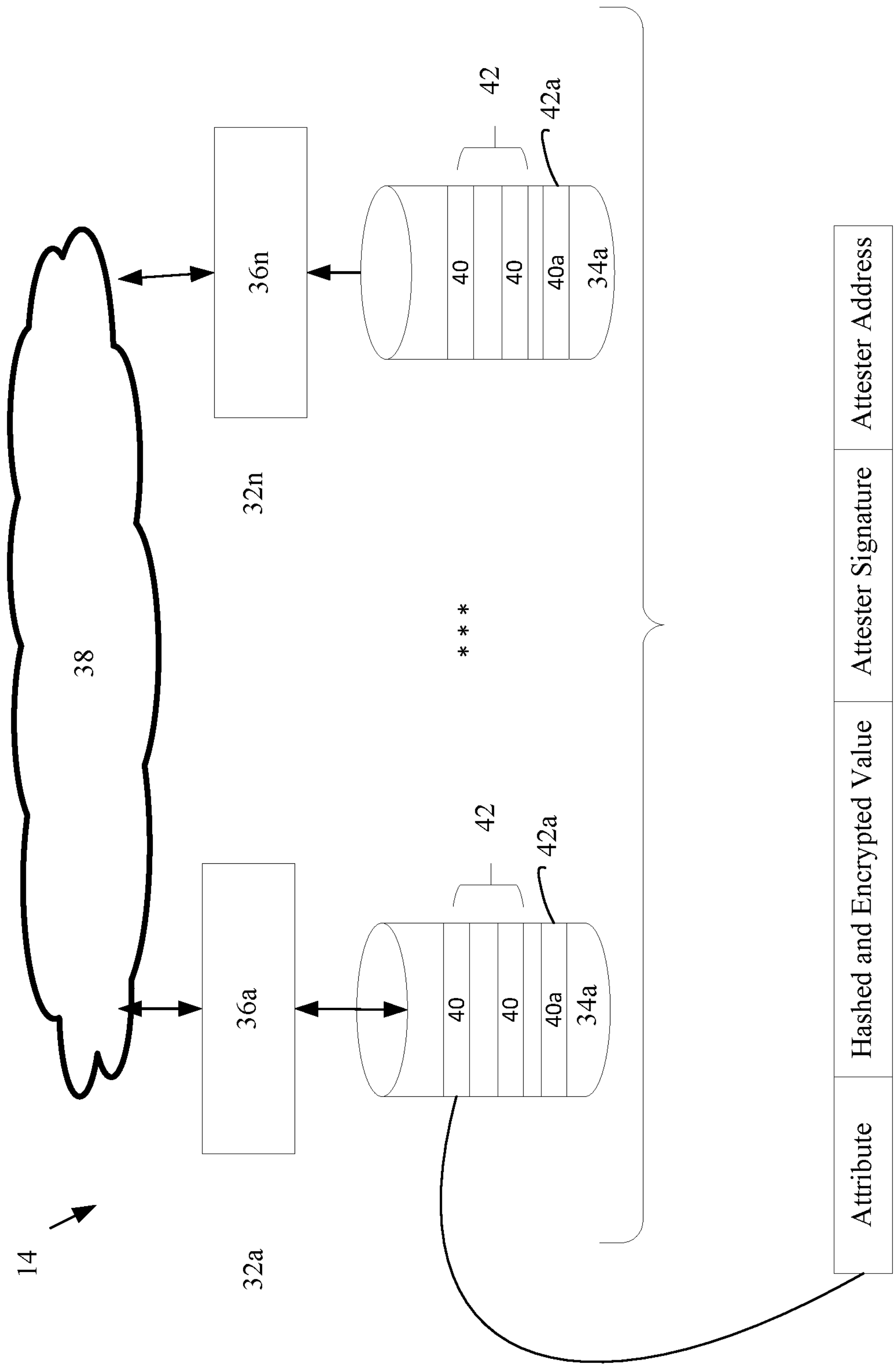

14
38
36a
36n
32a
32n
40
40
40a
34a
42
42a
* * *
Attribute
Hashed and Encrypted Value
Attester Signature
Attester Address

FIG. 5

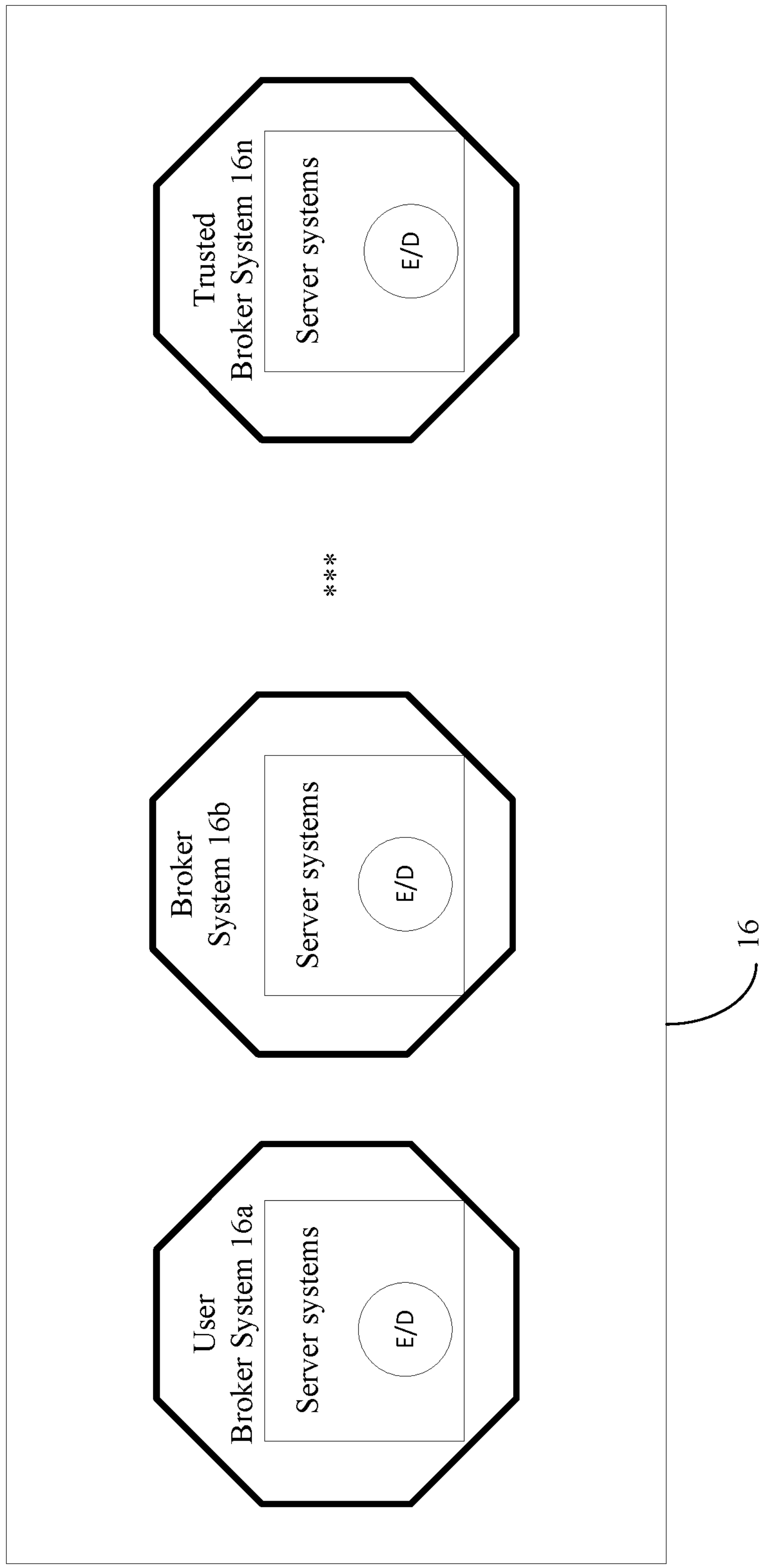

Trusted
Broker System 16n
Server systems
E/D
***
Broker
System 16b
Server systems
E/D
User
Broker System 16a
Server systems
E/D
16

FIG. 6

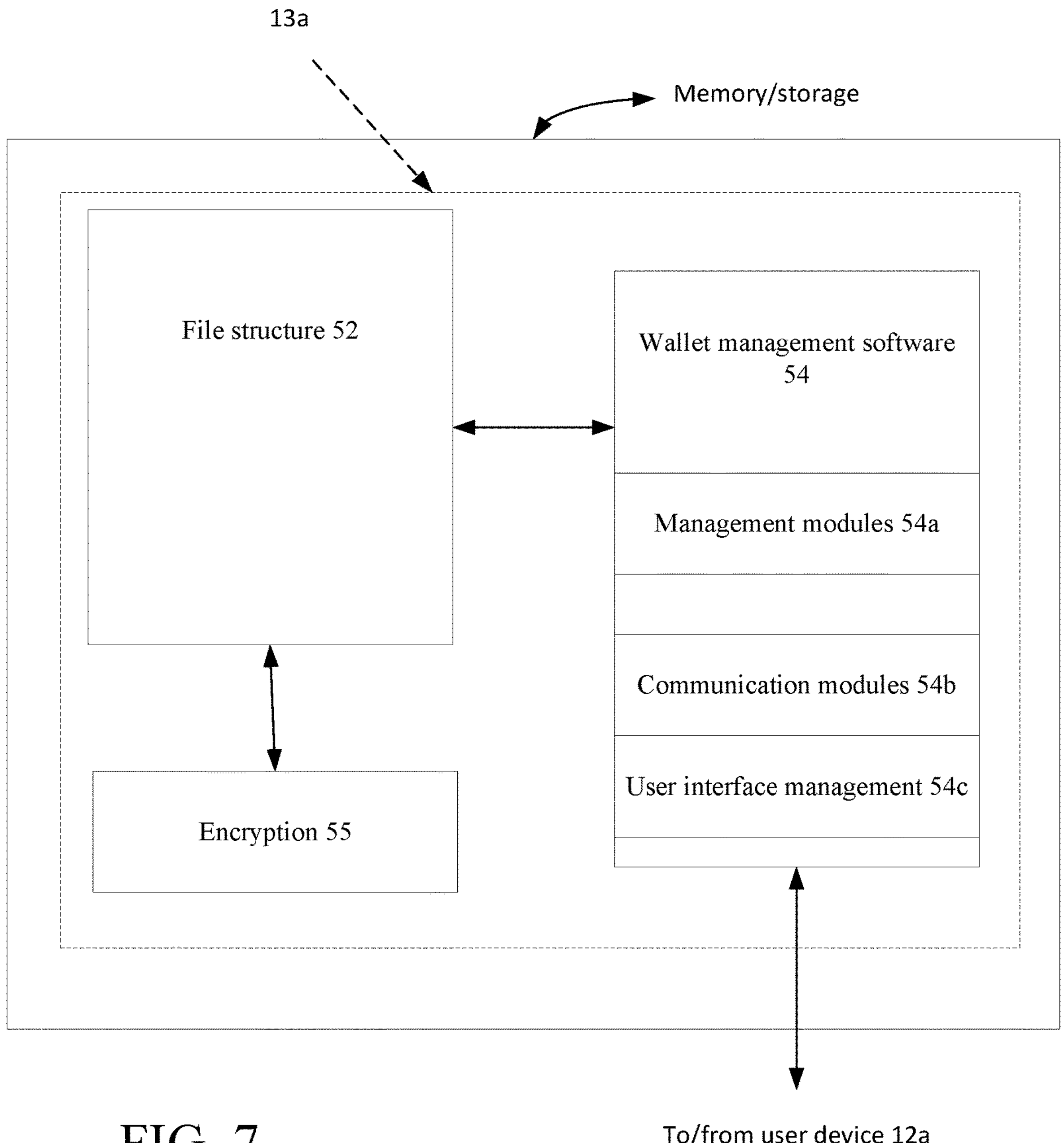

13a
Memory/storage
File structure 52
Wallet management software 54
Management modules 54a
Communication modules 54b
User interface management 54c
Encryption 55
To/from user device 12a

FIG. 7

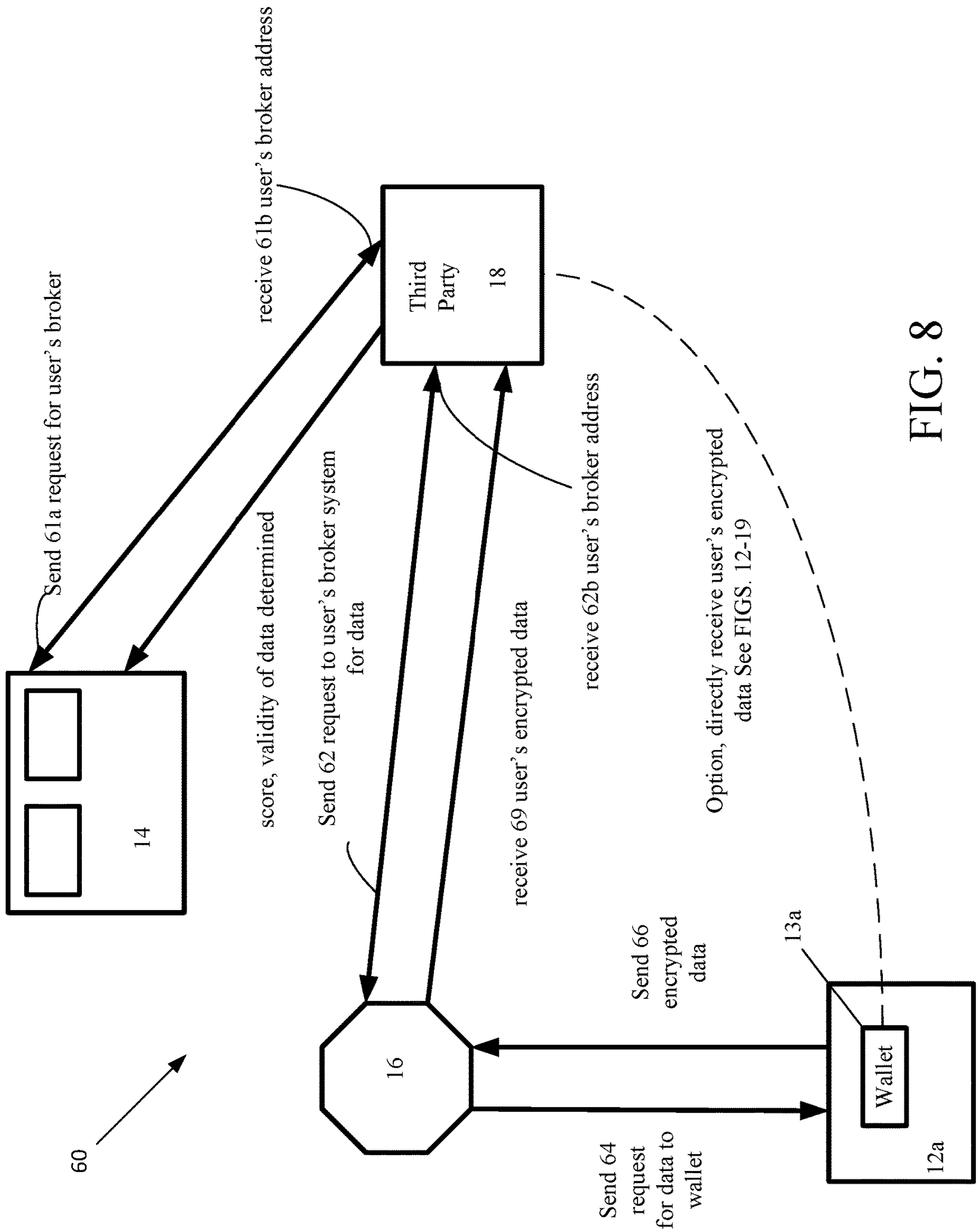

receive 61b user's broker address
Send 61a request for user's broker
Third Party
18
score, validity of data determined
Send 62 request to user's broker system for data
receive 69 user's encrypted data
receive 62b user's broker address
Option, directly receive user's encrypted data See FIGS. 12-19
14
16
60
Send 66 encrypted data
13a
Wallet
12a
Send 64 request for data to wallet

FIG. 8

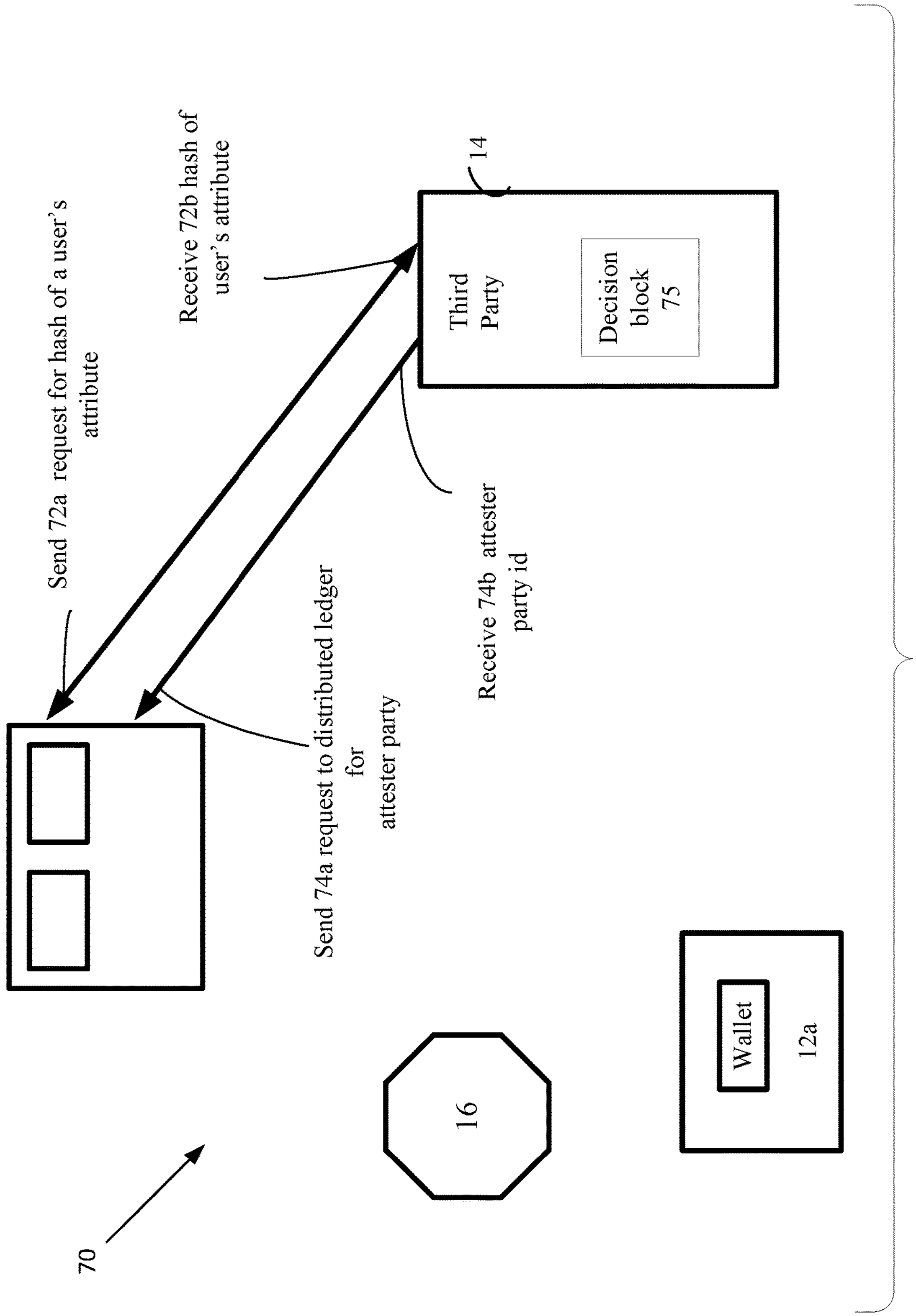

Send 72a request for hash of a user's attribute
Receive 72b hash of user's attribute
14
Third Party
Decision block 75
Receive 74b attester party id
Send 74a request to distributed ledger for attester party
70
16
Wallet
12a

FIG. 9

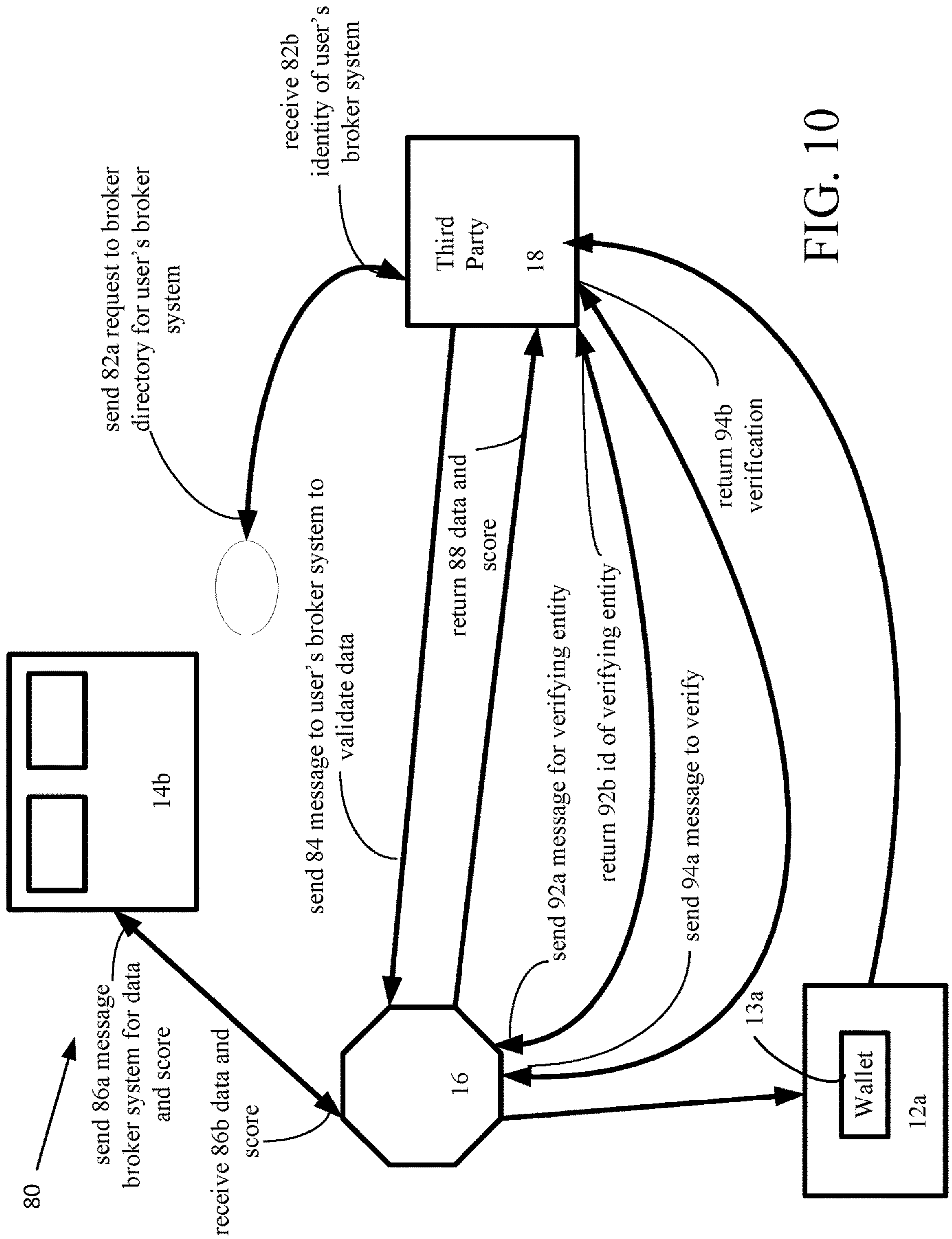

80
send 86a message broker system for data and score
receive 86b data and score
14b
16
send 82a request to broker directory for user's broker system
receive 82b identity of user's broker system
Third Party
18
send 84 message to user's broker system to validate data
return 88 data and score
send 92a message for verifying entity
return 92b id of verifying entity
send 94a message to verify
return 94b verification
13a
Wallet
12a

FIG. 10

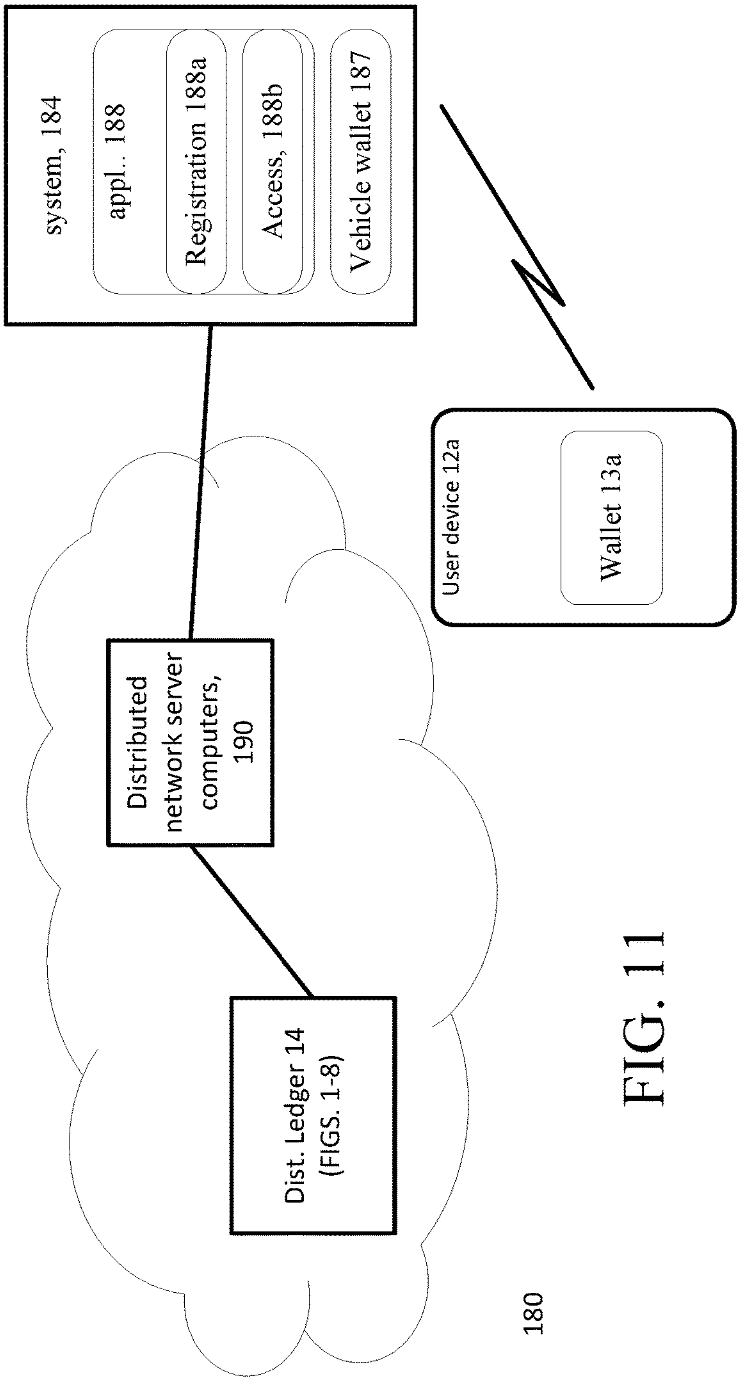

system, 184
appl.. 188
Registration 188a
Access, 188b
Vehicle wallet 187
User device 12a
Wallet 13a
Distributed network server computers, 190
Dist. Ledger 14 (FIGS. 1-8)
180

FIG. 11

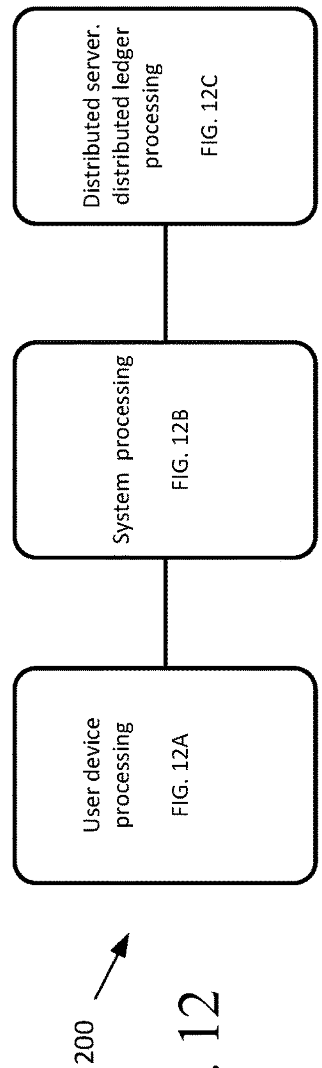

User device processing
FIG. 12A
System processing
FIG. 12B
Distributed server. distributed ledger processing
FIG. 12C
200

FIG. 12

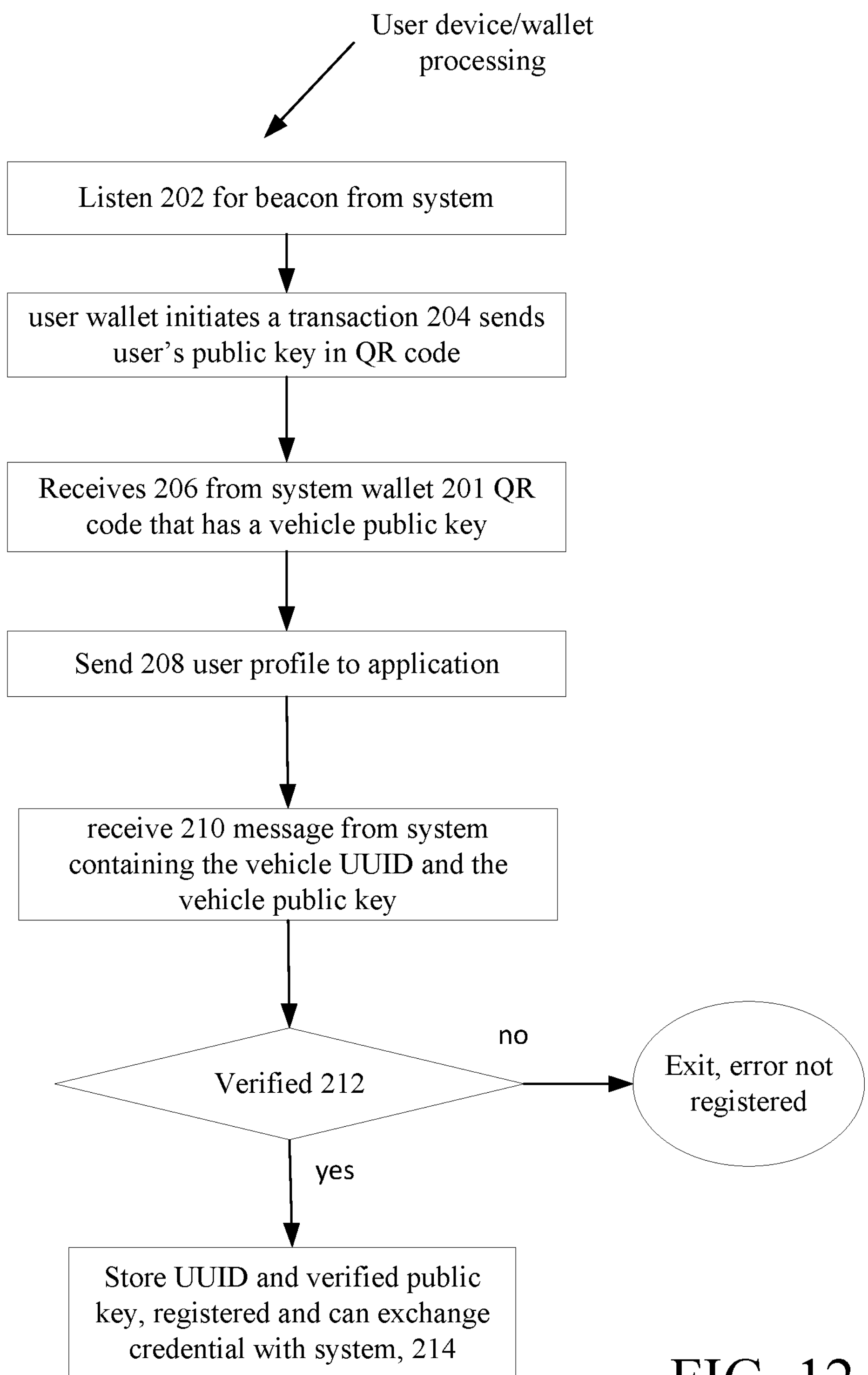

User device/wallet processing
Listen 202 for beacon from system
user wallet initiates a transaction 204 sends user's public key in QR code
Receives 206 from system wallet 201 QR code that has a vehicle public key
Send 208 user profile to application
receive 210 message from system containing the vehicle UUID and the vehicle public key
Verified 212
no
Exit, error not registered
yes
Store UUID and verified public key, registered and can exchange credential with system, 214

FIG. 12A

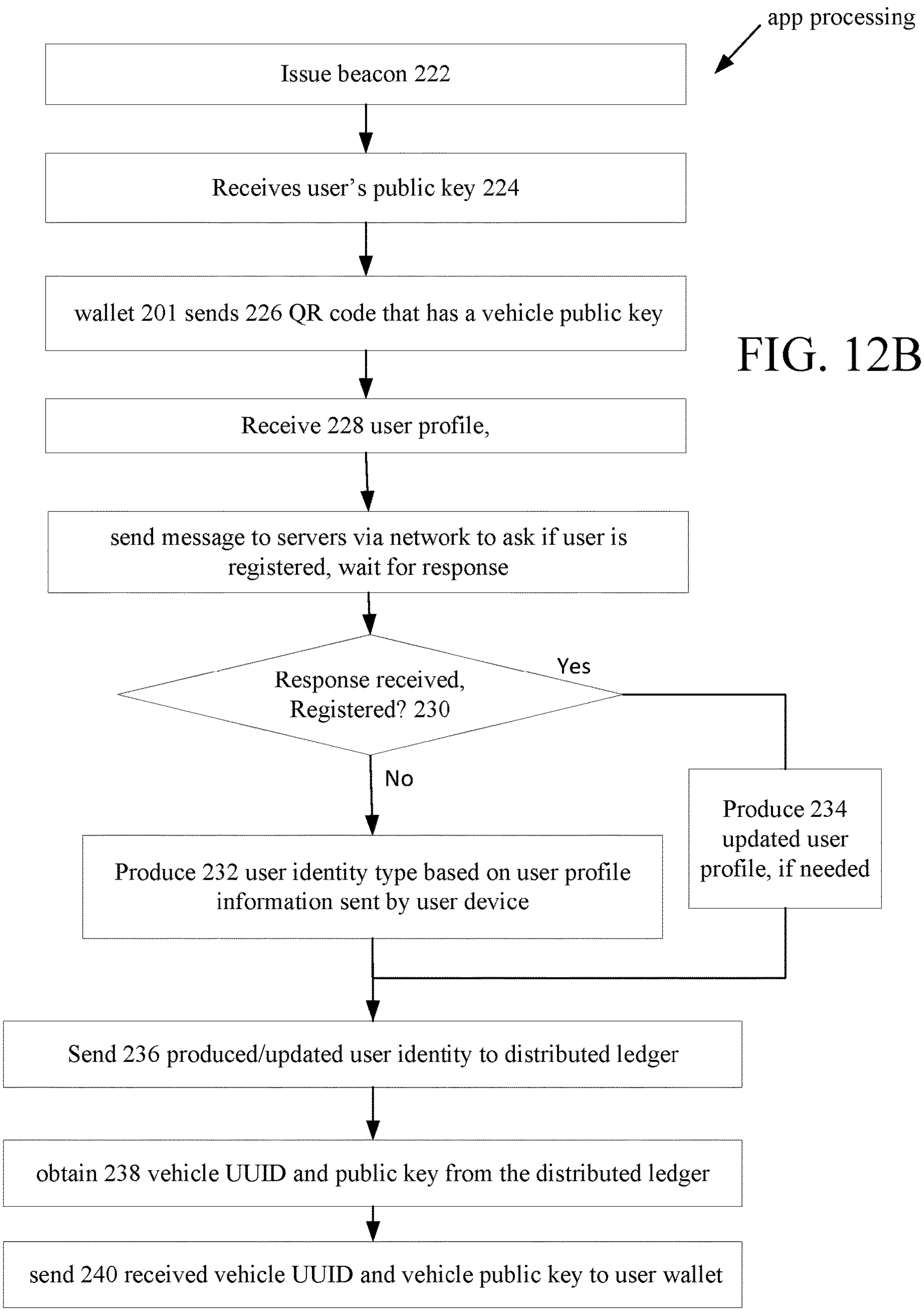

app processing
Issue beacon 222
Receives user's public key 224
wallet 201 sends 226 QR code that has a vehicle public key
Receive 228 user profile,
send message to servers via network to ask if user is registered, wait for response
Response received, Registered? 230
Yes
No
Produce 234 updated user profile, if needed
Produce 232 user identity type based on user profile information sent by user device
Send 236 produced/updated user identity to distributed ledger
obtain 238 vehicle UUID and public key from the distributed ledger
send 240 received vehicle UUID and vehicle public key to user wallet

FIG. 12B

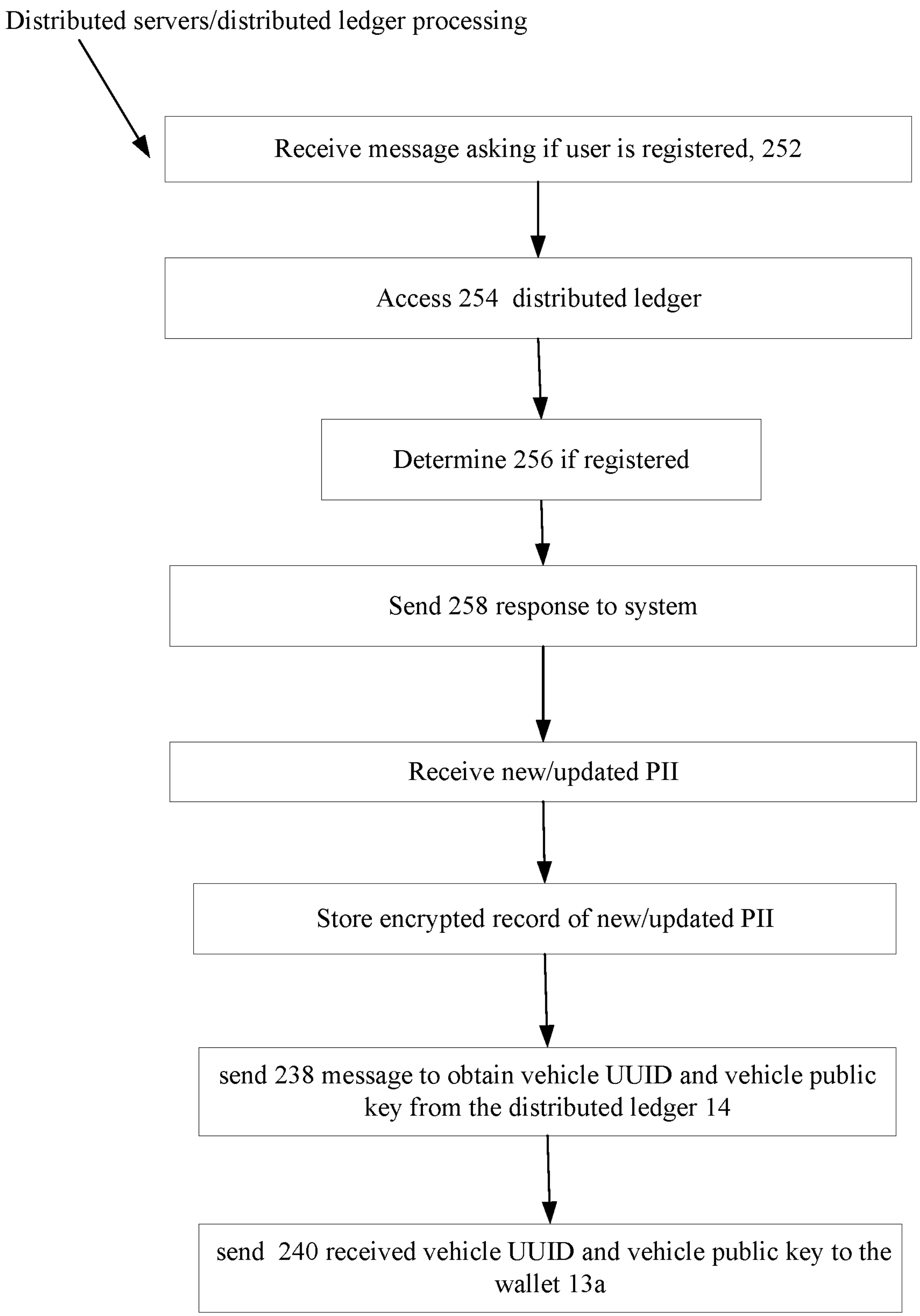

Distributed servers/distributed ledger processing
Receive message asking if user is registered, 252
Access 254 distributed ledger
Determine 256 if registered
Send 258 response to system
Receive new/updated PII
Store encrypted record of new/updated PII
send 238 message to obtain vehicle UUID and vehicle public key from the distributed ledger 14
send 240 received vehicle UUID and vehicle public key to the wallet 13a

FIG. 12C

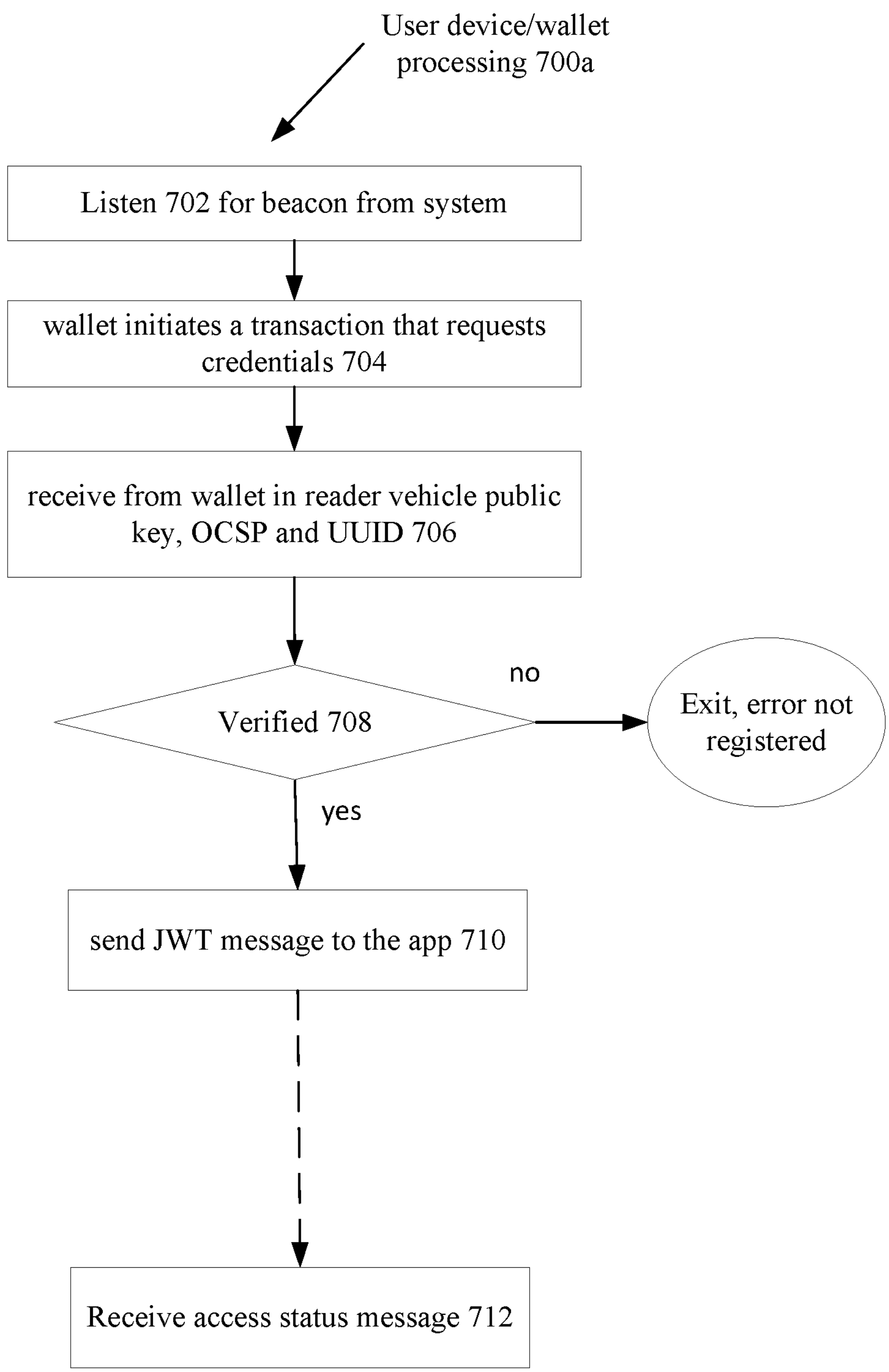

User device/wallet processing 700a
Listen 702 for beacon from system
wallet initiates a transaction that requests credentials 704
receive from wallet in reader vehicle public key, OCSP and UUID 706
Verified 708
no
Exit, error not registered
yes
send JWT message to the app 710
Receive access status message 712

FIG. 13A

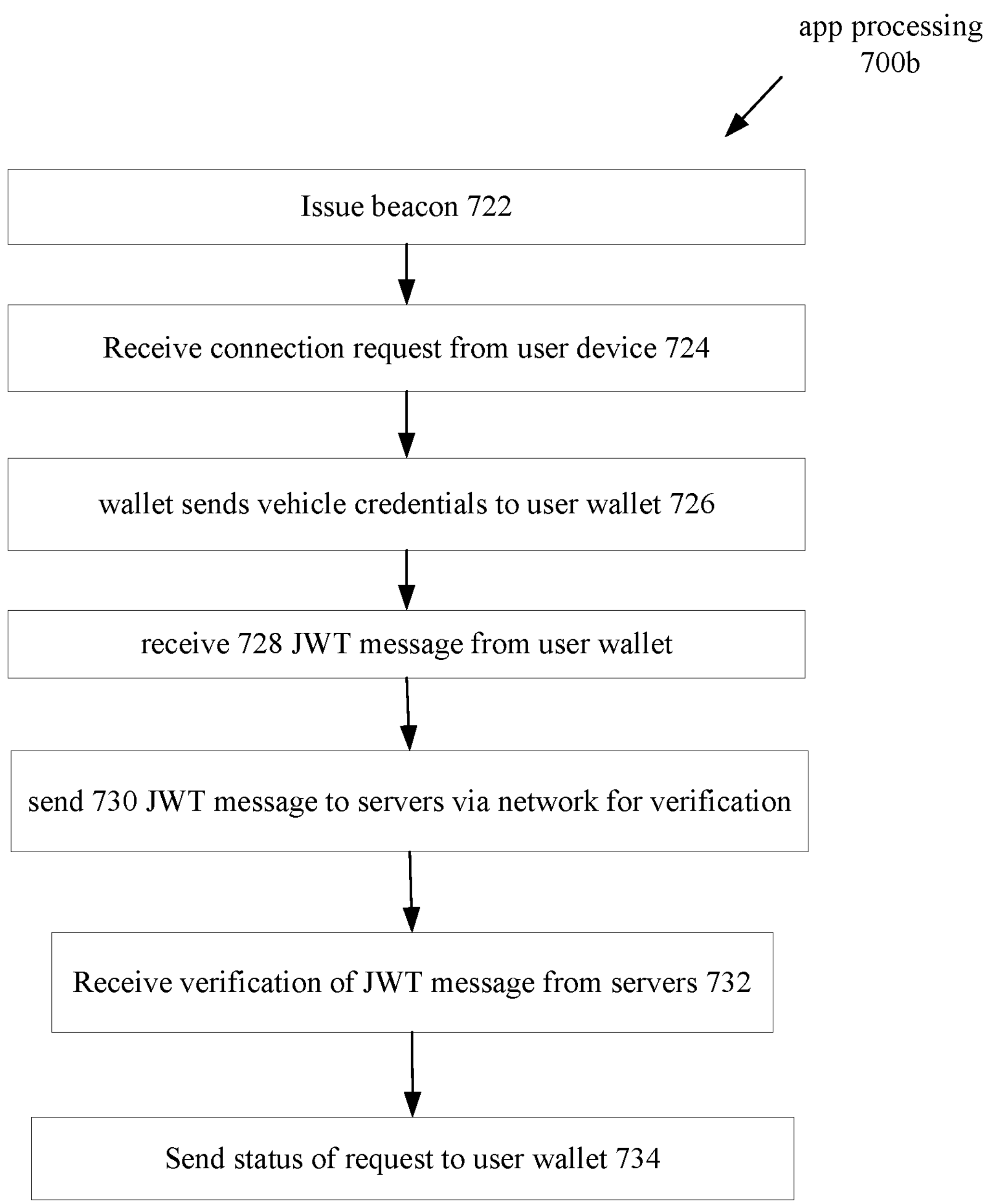

app processing
700b
Issue beacon 722
Receive connection request from user device 724
wallet sends vehicle credentials to user wallet 726
receive 728 JWT message from user wallet
send 730 JWT message to servers via network for verification
Receive verification of JWT message from servers 732
Send status of request to user wallet 734

FIG. 13B

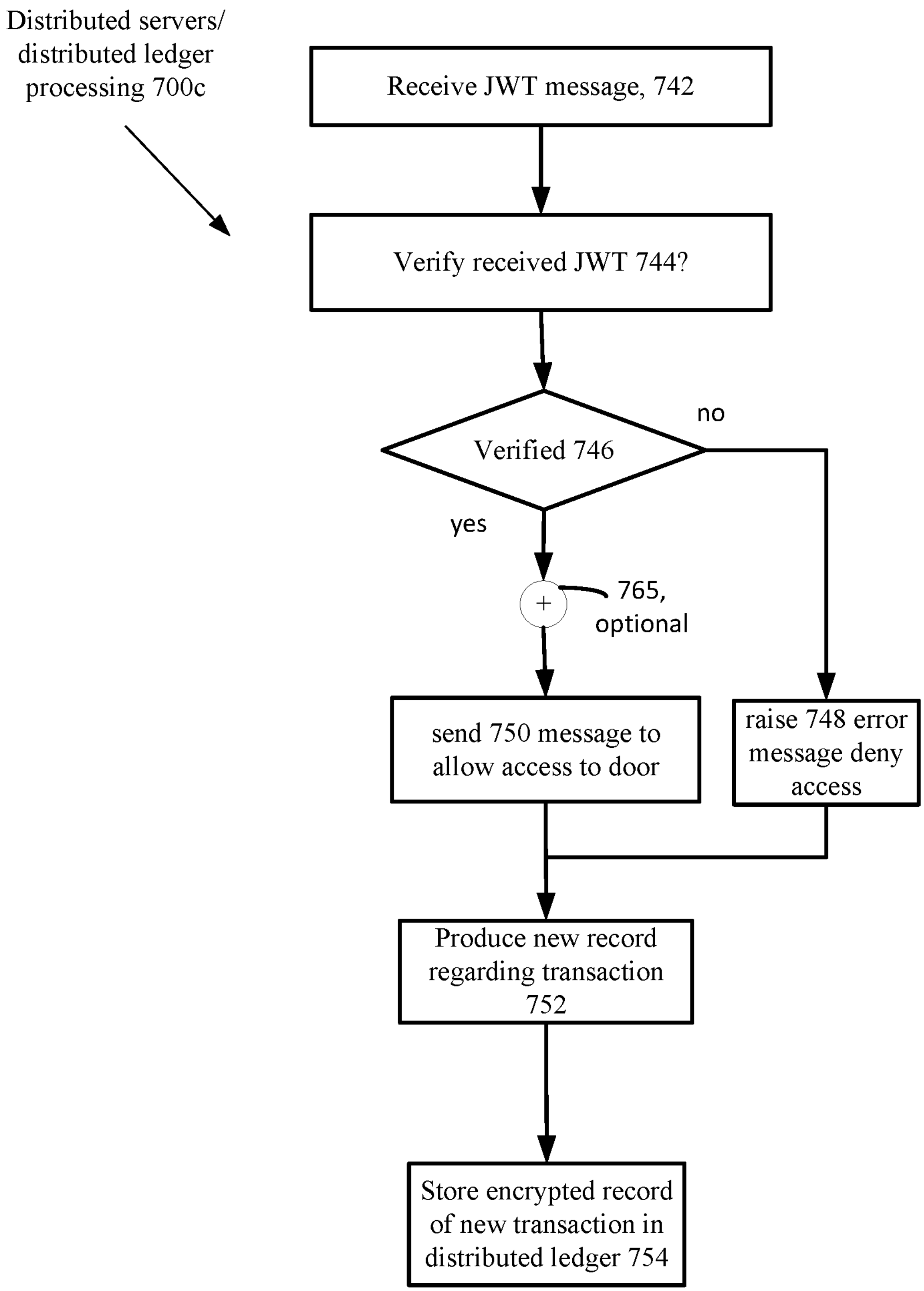

Distributed servers/
distributed ledger
processing 700c
Receive JWT message, 742
Verify received JWT 744?
Verified 746
no
yes
765,
optional
send 750 message to
allow access to door
raise 748 error
message deny
access
Produce new record
regarding transaction
752
Store encrypted record
of new transaction in
distributed ledger 754

FIG. 13C

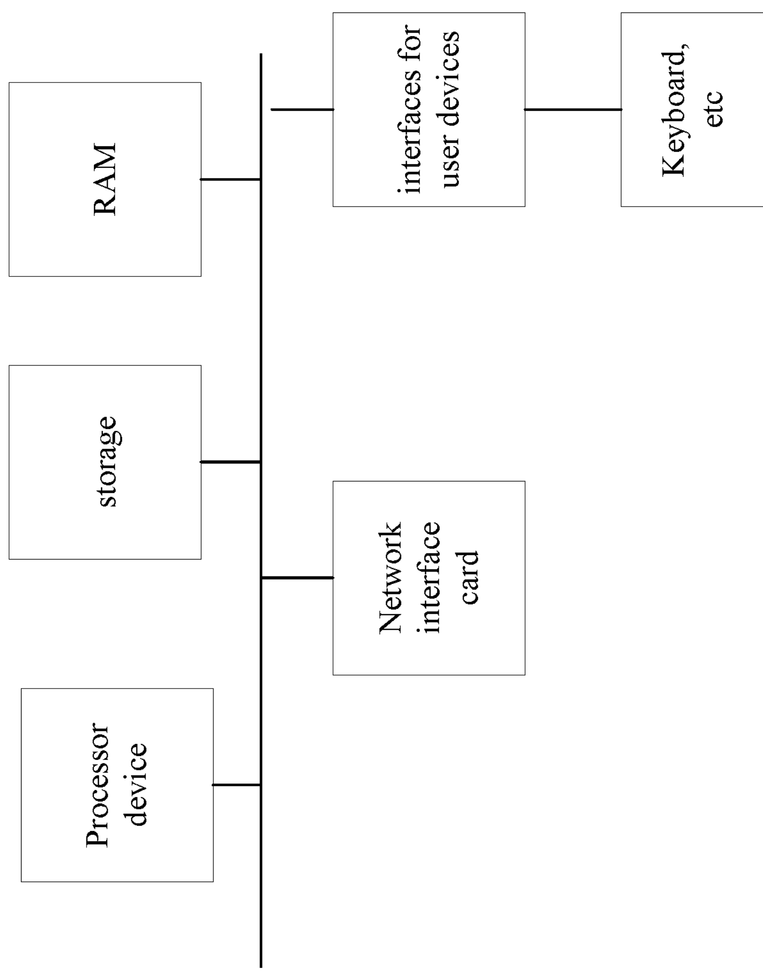

RAM
storage
Processor device
interfaces for user devices
Keyboard, etc
Network interface card

FIG. 14

IDENTITY MANAGEMENT FOR IMPLEMENTING VEHICLE ACCESS AND OPERATION MANAGEMENT

CLAIM OF PRIORITY

This application claims priority under 35 U.S.C. § 119(e) to provisional U.S. Patent Application 62/561,743, filed on Sep. 22, 2017, entitled: "Methods and Apparatus for implementing Identity and Access Management," the entire contents of which are hereby incorporated by reference.

BACKGROUND

This description relates to operation of networks for dissemination of information for vehicle access and operation.

Access control systems commonly employ access cards or physical keys or physical fobs that include corresponding embedded electronic credentials that are read by a corresponding reader. Access to a motor vehicle for instance merely requires possession of a physical key (with or without embedded credentials).

It is common for computer systems to gather information, such as proprietary data on individuals. One type of information is proprietary data such as "personally identifiable information" commonly referred to as "PII." PII is information of a sensitive, personal nature that is generally associated with individuals and is often protected by privacy laws in many jurisdictions. PII is information that can identify or contact or locate a single person or to identify an individual in context. Examples of PII include name, social security number, date and place of birth, mother's maiden name, biometric records and information that is linkable to an individual, such as medical, educational, financial, and employment information, as well as a user's device IP address used in a communication service broker.

Another type of information is proprietary data such as Machine Identifiable Information or "MII," such as in the context of the "Internet of Things." That is, other information that is collected includes operational information such as information used to control access control systems, intrusion detection systems and integrated security/alarm systems. For different reasons each of these types of information may have a sensitive nature that should limit the ubiquitous retention of such information in disparate systems.

Modern information technology and the Internet have made it easier to collect PII and MII through various mechanisms leading to various problems such as aiding of criminal acts, identity theft, etc.

Various systems employed in vehicles contain dedicated microprocessors that run firmware to measure various parameters. For example, battery products are ever increasingly containing microprocessors that run firmware to measure battery load, voltage, temperature etc. and communicate directly with the main vehicle computer system.

SUMMARY

The techniques described herein provide a higher level of identity validation that will be required as access management services are expanded to encompass a greater range of functionality. The described architecture provides validation of the person who is in possession of an identity item as opposed to merely validating the item itself.

According to an aspect, a method includes receiving an electronic representation of a user's identity, by a vehicle access application executable in a computing system in the vehicle, sending by the computing system to an identity and access management system the received electronic representation of the user's identity, receiving by the computing system from the identity and access management system credentials that validate the electronic representation of the user's identity, and enabling by the computing system starting of the vehicle when the computing system receives the credentials that validated the user's identity.

Aspects also include computer program products and methods. Additional features of the computer program product, systems and methods include other features disclosed herein.

One or more of the above aspects may provide one or more of the following advantages.

In some implementations, these aspects enable user devices to transmit PII (and other confidential information) without that information being hosted by third party (requesting systems) that would otherwise manage and store such PII (and other confidential information). In other implementations information can be hosted by third party systems or such information can be held by third party systems for attestation purposes, e.g., a registry such as a motor vehicle registry.

Currently third party requester systems are ubiquitous, but the techniques currently employed make such information vulnerable to improper access and disclosure through various types of hacking attacks on any of the ubiquitous numbers of third party requester systems.

The disclosed techniques including an application that in conjunction with the distributed ledgers can send to user devices containing a wallet a verified access or access error depending on the outcome of processing. All exchanges are logged in the distributed ledger for audit tracking, etc. and verification of information can be used with information in the distributed ledger. Records are added to the distributed ledger as transactions and include a hashed record of the transaction, what was exchanged, the signatures of the parties, and may include additional detailed information depending on the type of distributed ledger used.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention is apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

FIG. **1** is a schematic diagram of an exemplary system for securing PII information.

FIG. **1**A is a schematic diagram of an exemplary system for vehicle access and operation management employing a PII system such as FIG. **1**.

FIG. **1**B is a flow diagram of P-II-based vehicle access and operation management processing.

FIGS. **2**-**4** are flow diagrams of vehicle access and operation management processing.

FIG. **5** is a block diagram of a distributed ledger.

FIG. **6** is a block diagram of a broker system.

FIG. **7** is a block diagram of an identity wallet.

FIGS. **8**-**10** are block diagrams for message exchange processes.

FIGS. **11** and **12** are block diagrams.

FIGS. **12**A-**12**C and **13**A-**13**C are flow diagrams.

FIG. **14** is a block diagram of an exemplary device/system.

DETAILED DESCRIPTION

Described herein is use of an IAM system (Identity and Access Management) for vehicle access verification. The IAM system includes a set of techniques that provide a solution using a private service broker for dissemination of information such as PII (as well as other confidential information) between two or more electronic devices. The dissemination of information occurs in a controlled, secure and confidential manner. Also described is a mechanism that allows for the verification of information including PII (as well as other confidential information), and credentials, without the actual disclosure of the PII (as well as other confidential information).

The vehicle access verification system described uses a combination of an identity wallet that executes on a user device, a distributed ledger that manages proxies for PII (as well as other confidential information), along with a service broker system that securely manages data transmissions and verifications of the data without actually having the wallet directly access the distributed ledger. In some implementations the service broker is not needed.

Referring now to FIG. **1**, an exemplary distributed network IAM system **10** (system **10**) for access control and identity credential verification is shown. Approaches as discussed in detail in below use an Identity Wallet **13***a*, **13***b* with a distributed ledger **14** back-end that replaces the typical centralized database (not shown). The ID Wallet/distributed ledger approach provides enhanced user experience, security, compliance and so forth, as discussed below. The ID Wallet can replace and/or complement a conventional physical access key or ignition key.

The system **10** includes user devices, here wireless enabled user mobile devices, such as smartphones **12***a*, **12***b* that house respective identity wallets **13***a*, **13***b*. The smartphones **12***a*, **12***b* house the identity wallets (also referred to herein simply as wallets) **13***a*, **13***b*, respectively and thus carry user credentials and by use of the wallet and a processor on the smartphone, interacts with portions of the access control system **10**.

The term "smartphone" is used to describe a mobile phone device that executes an advanced mobile operating system. The smartphone has hardware and a mobile operating system with features of personal computer hardware and operating systems along with features required for mobile or handheld operation, such as those functions needed for use of the smartphone as a cell phone and includes GPS (global position system) navigation. The smartphone executes applications (apps) such as a media player, as well as browsers, and other apps. Smartphones typically can access the Internet and have a touchscreen user interface. Other types of user devices could be used including personal computers, tablet computers, as well as, systems that are involved with exchange of sensitive data, such as access control systems and intrusion detection systems.

Other form factors can be used to house the identity wallet **13***a* such as wearables. Other aspects of identity can include biometrics. For illustrative purposes, the discussion will focus on the user devices **12***a*, **12***b* as being smartphones. The identity wallets **13***a*, **13***b* are housed in the smartphones. As used herein an identity wallet includes an application that executes on an electronic device, such as the user devices **12***a*, **12***b*, and which allows a user of the device to store identity information, encrypt such identity information and communicate with external systems via communication functions/circuitry on the smartphone.

Identity Wallets **13***a*, **13***b* are also used to authenticate credentials of the holder of the particular wallet, as well as other wallets and other systems/devices, as will be discussed below. The term "wallet" encompasses an arrangement of three major systems, an electronic infrastructure, an application that operates with the system and the device (e.g., smartphone) that holds the wallet. In the discussion below, the holder's proprietary data is associated with the wallet. For example, many pieces of identifying information can be stored in the wallet.

Such information can be diverse and wide-ranging, such as, bank account information, as well as the holder's information such as driver's license, health records, health care, loyalty card(s) and other ID documents stored on the phone, social security no., etc. All of this information can be stored in some manner and/or linked to the wallet. In particular stored in this wallet are pieces of information identifying the holders credentials, etc. Systems are broadly defined as mechanical, electromechanical, and electronic systems, such as computers. Many of such systems will have a component of which is computer controlled. Software is defined as the programming code tangible stored and residing in an electronic machine, such as a computer system, and which coded is executable or executing under normal conditions.

In the discussion below, in particular, the wallet **13***a* holds a user's credentials. One type is the user's credentials that are needed for access to the vehicle.

The system **10** also includes a distributed ledger system **14**. The distributed ledger system **14** is a sequential, distributed transaction database. An example of a sequential, distributed transaction database is the so-called "Blockchain" that operates with cryptocurrencies, such as "bitcoin"® (bitcoin project.org). The distributed ledger **14** rather than being dedicated to managing cryptocurrencies, manages PII transactional records and other types of records, rather than cryptocurrencies, and serves as the backend for a distributed access and verification system. The distributed ledger system **14** interacts with the user's wallet as well as third party systems to register user's and allow user access to the vehicle. While sharing some similarities to the Blockchain as well as other known types of sequential transaction databases, the distributed ledger **14** has some significant differences.

Accordingly, the distributed ledger **14** has a structure as set out below. In some implementations of the distributed ledger **14**, the system **10** also includes a service broker system **16** that is a third party service system that interfaces between the wallet **13***a* and the distributed ledger **14**. In other implementations, the service broker system **16** is not needed.

From the distributed ledger **14** encrypted PII data upon request are transmitted to third party systems, as well as sending to third party systems listings of verifying systems, upon receiving access requests from the third party system. The service broker includes a hardware platform. For example, with a self-contained enterprise example, the Service Broker would include a hardware platform (e.g., a server computer system), a server operating system and a "calculator/attester algorithm" (discussed below). The "calculator/attester algorithm" would broker between the source and target peer-to-peer entities such that a minimal amount of information required to legitimize and execute an information exchange between the source and target is determined, exchanged, and validated so that a "transaction" can occur. The record of the transaction is written into the distributed ledger **14** with the minimum amount of PII or MII information, if any, including any metadata regarding the transaction or the information

The system **10** also includes external systems **18**. In some examples these external systems **18** are third party systems **18***a*. The third party system **18***a* can be any electronic system (or device) and is the system/device that seeks some aspect of the PII or other confidential information of a user or held by the user device **12***a*, associated with the user. In the examples discussed below the external systems can be registration systems **18***b*, in other examples the external systems can be motor vehicles to permit physical access as well as control (starting) of the vehicle. By physical access is meant access to a physical item, such as a motor vehicle, e.g., car, truck, etc. In the processes discussed below, some or all of the aforementioned user device **12***a*, wallet **13***a*, distributed ledger **14**, optionally service broker **16** and third party access system **18** are used.

Driver Management

Various systems employed in vehicles contain dedicated microprocessors that run firmware to measure various parameters. For example, battery products are ever increasingly containing microprocessors that run firmware to measure battery load, voltage, temperature etc. and communicate directly with the main vehicle computer system.

Referring now to FIG. **1**A, a networked arrangement **20** for monitoring vehicle access and operation is shown. The arrangement **20** will be described in reference to accessing of a motor vehicle **21** such as a car. The arrangement involves vehicle electronic control equipment **21***a* that includes access control systems **22***a*, other vehicle systems such as those that monitor vehicle operation and environmental systems (not shown), ignition systems **22***b* to start the vehicle, and potential driver-testing devices **22***c* that test the status of the potential driver. Examples of potential driver-testing devices **22***c* include breathalyzer devices that analyze a potential driver's breathe to test the level of intoxication of the potential driver. Other potential driver testing devices **22***c* can be devices that measure an extent of other types of potential driver impairments to safe operation of the vehicle.

The arrangement **20** uses the distributed network IAM system **10** (FIG. **1**) for access control to a vehicle. The arrangement **20** includes user devices **12** that are carried by the user that act as, e.g., a "virtual key" for entry into the vehicle. In the discussion below, an external system **18***a* is configured to determine whether a given user has privileges or authorization to enter and operate the vehicle. The arrangement also includes a specific one **12***a* of the user devices (generally **12**) that houses the digital wallet (wallet) **13***a*, as discussed in FIG. **1**.

Referring now to FIG. **1**B, an overall view of an embodiment **19** of the IAM system **10** used in conjunction with the vehicle **21**, e.g., automobile is shown. When a potential driver enters the vehicle **21**, the driver presents **19***a* his/her identity to the vehicle. The identity is presented through a wireless connection between an application on a user device such as the smartphone **12***a* to the IAM system **10**. In one embodiment, the application is an identity wallet **13***a* on the smartphone **12***a*. A system executing an application on a vehicle computer (either the main computer system or another system such as a battery system), in the vehicle receives **19***b* credentials from the user device and connects **19***c* to the IAM system via an Internet connection. Examples of requested information include birth date, driver license number, home address etc. The IAM system is a specific implementation of a cloud based service that validates the driver's identity and whether the driver is authorized to drive the vehicle. This could be used, as one example, when employees of a company can only use the vehicle during specified hours on specified days and also determines the driver's identity, if the driver has the requisite training to operate the class of vehicle.

The application on the vehicle computer receives **19***d* from the IAM system a decision regarding validation of the received credentials of the driver. If acceptable **19***e*, the application in one embodiment will engage **19***f* with the ignition system of the vehicle to allow the driver to start the vehicle (shown as a dashed line). If not acceptable **19***g* the application will engage with the ignition system of the vehicle to block starting of the vehicle.

In some implementations, sensors can be deployed to sense presence of intoxicants **19***h* (alcohol or drugs, such as marijuana, etc.). That is, the system (either the main computer system or another system such as a battery system), in the vehicle can also be coupled to other sensors that gather data to be used to ascertain whether the potential driver is fit to drive the car. One example of such a sensor is a sobriety checking sensor. If impaired **19***i* application will lock the ignition system **19***g*. Otherwise, if not impaired, the application will engage **19***f* with the ignition system of the vehicle to allow the driver to start the vehicle (shown as dashed lines).

Thus, if the system determines that the driver is not authorized or is incapable of operating the car, the system will not start the car. In one particular example, the battery system determines fitness and will not provide power to start the engine should the potential driver be ascertained as unauthorized or unfit.

Referring now to FIG. **2**, a specific implementation **24** of the networked arrangement **20** for monitoring vehicle access is shown. In this arrangement, the vehicle is a rental vehicle and rental arrangements are made via an on-line transaction **24***a*. The details of the actual on-line transaction are not included in this discussion, as for the most part the details of the actual on-line transaction would be similar to those for conventional rental of a vehicle where a user presents a license, etc. at a rental agency counter. Suffice it here to say that the transaction includes a user making a reservation for a vehicle, paying for the vehicle via a credit card or other mode such as a virtual currency, e.g., Bitcoin, Ethereum, etc.

However, as part of the transaction upon completion of the reservation of the rental vehicle the arrangement either presents **24***b* a list of authenticating items that the potential driver will need to present electronically when the potential driver picks up the vehicle.

In an implementation that will be discussed in detail, below part of the transaction includes a registration process **24***c* to establish via the registration process **24***c* verified personal authenticating items in the potential driver's wallet. As part of the registration process **24***c*, (discussed in FIG. **3**) the potential driver's device **12***a*, e.g., wallet **13***a* shares **24***c* with the IAM system **10** (FIG. **1**), personal information that is validated **25***b* by the IAM system (i.e., with entities that are part of the distributed ledger **14** such as, for example, a governmental entity). Authenticating items will generally include a driver's license and/or one or more credit cards, including a credit card that the potential driver carries and which was used to pay for the rental, or in the case of use of a virtual currency a transaction record associated with the use of the virtual currency with payment of the rental and birth date, driver license number, home address etc. Other authenticating items could be used.

When a potential driver enters (or arrives at) the vehicle, the potential driver presents his/her identity to the vehicle through a wireless connection between an application on a potential driver device such as the smartphone **12***a* to the IAM system **10**. The arrangement **24** uses the motor vehicle's **21** vehicle electronic control equipment **21***a* that includes the access control system **22***a*. The access control system includes in addition to conventional vehicle access systems, a credential reader (via wireless near field device technology) that reads **24***d* potential driver credentials in the user wallet **13***a* (in contrast to reading a manually entered code, or a code embedded in a physical key or a physical fob which are dedicated to such function, etc.). The identity wallet **13***a* on the smartphone **12***a* connects to a system in the vehicle, which executes an application. The system is in the vehicle. The system can be the main computer system or another system such as a battery system that includes a computing device. The system reads **24***d* the credentials from the potential driver device and connects to the IAM system **10** via an Internet connection and sends the read credentials for verification.

The system in the vehicle receives results **24***f* of the verification request from the IAM system **10**. Upon verification **24***f* of credentials supplied by the potential driver's the arrangement **24** controls the ignition system **22***b* to allow the potential driver to enter and to start the vehicle. Upon entering the arrangement **24** can also use the motor vehicle's **21** vehicle electronic control equipment **21***a* to interface **24***g* with optional potential driver-testing devices **22***c* that test **24***h* the status of the potential driver. Either one or both can be used to controls the ignition systems **22***b* to allow the potential driver to start the vehicle. Also, verification can be used to allow the potential driver to merely start the vehicle or to enter and start the vehicle depending on implementation. Upon failure of verification **24***i* of credentials supplied by the potential driver's the arrangement **24** controls the ignition system **22***b* to allow the potential driver to enter and to start the vehicle.

Registration

Referring now to FIG. **3**, the registration process **24***c* (FIG. **2**.) uses the distributed network IAM system **10** (FIG. **1**) to verify credentials in the user's wallet **13***a*, which effectively loads onto the user device **12** a key for entry into and starting of the vehicle. In the discussion below, an external system **18***a* is configured to determine whether a given potential driver has privileges or authorizations to enter and operate the vehicle. The arrangement also includes the user device **12***a* that houses the digital wallet (wallet) as discussed in FIG. **1**. This registration process **26** could also be used at the time of potential driver arrival at the vehicle to satisfy the requirement of authenticating credentials that the potential driver will need to present electronically (see **24***b*, FIG. **2**).

The potential driver can register, e.g., pre-register, with a system that performs rental and verification processing for a rental agency. Pre-registration can be before during or subsequent to completion of a rental transaction. As part of pre-registration, the potential driver's device **12***a*, e.g., wallet **13***a* shares **25***a* with the IAM system **10** (FIG. **1**), personal information that is validated **25***b* by the IAM system (i.e., with entities that are part of the distributed ledger **14** such as, for example, a governmental entity). If validated **25***d*, the process **24***c* causes a download **25***d* of a mobile application to their device, e.g., smartphone **12***a* and the process tests **25***d* if a transaction was generated. If a transaction was not generated, the process **24***c* waits till the transaction is generated (or the process **24***c* can exit or take other action). When the transaction is generated, a QR code, or other electronic code is sent **25***e* to the potential driver's device **12***a* and/or wallet **13***a*. The QR code or other electronic code will include identifying code of the vehicle used for the rental transaction, as well as a location of the vehicle, description, etc.

Referring now to FIG. **4**, at check in the potential driver scans **27***a* the QR code or processes the electronic code. From the scan of the QR code (or processing of the electronic code) the device receives **27***b* credentials of the vehicle. The credentials of the vehicle are scanned and compared to credentials of the vehicle reserved for the user. If there is a match the user can share its credentials.

The device also receives **27***c* the listing of the personal information required. If the potential driver had not previously registered the wallet with its credentials with the system **27***d*, the listing will be displayed to the potential driver and will allow the user device upon verification of the credentials of the vehicle by the user device to release the personal information required from the user wallet. The system will send **27***e* the authenticating items to the IAM system **10**. The process of FIG. **3** could be used/adapted for this verification.

If verified **27***f*, or if the potential driver had registered the wallet with its credentials with the system, e.g., during the transaction (FIG. **2**, **24***c*), the wallet **13***a* (user device **12***a*) sends **27***g* the credentialed code to the vehicle. If the code is verified (FIG. **2**, **24***e*), verification of the codes causes the vehicle to be unlocked and allows the potential driver to start the vehicle (e.g., pushbutton starting). If there is neither a match at **27***c* or verification at **27***f*, the process can exit, indicate an error or take other action **27***h*. In either case, release of personal information is according to the processes described below.

As mentioned, in some implementations sensors are deployed and sensor process (shown in phantom for both cases) is executed to sense presence of intoxicants (alcohol or drugs, such as marijuana, etc.) (see **19***h*, FIG. **2**). That is, the system (either the main computer system or another system such as a battery system), in the vehicle ascertains whether the potential driver is fit to drive the car, as discussed above. Thus, if the system determines that the driver is not authorized or is incapable of operating the car, the system will not start and/or unlock the car, as appropriate.

Referring now to FIG. **5**, the distributed ledger system **14** is shown. As mentioned, the distributed ledger system **14** is a sequential, distributed transaction database. The distributed ledger system **14** thus includes distributed databases **32***a*-**32***n* that are typically existing in the "Cloud." The distributed database comprise storage devices **34***a*-**34***n* that are attached to different interconnected computers **36***a*-**36***n*. The distributed databases are controlled by a distributed database management system that controls storage of data over a network **38** of the interconnected computers and execute corresponding replication and duplication processes. Replication software (not shown) detects changes in the distributed database contents and once the changes have been detected, replicates the changes to have all the databases the same. Duplication software (not shown) identifies one database (not shown) as a master and then duplicates that database across other databases. Replication and duplication keep the data current in all distributed storage locations.

Each of the distributed databases **32***a*-**32***n* that form the distributed ledger system **14** store encrypted information records. Typically the records will be a hash of an information record or a hashed pointer to an information record. In theory, assuming that the distributed databases **32***a*-**32***n* could be hacked, a hacker will not access the actual data in information records, but only a hash of the actual data. An exemplary record **40** is shown below. The record **40** is stored in each of the distributed databases **32***a*-**32***n* that form the distributed ledger system **14**, which stores the record **40** in an encrypted form in the distributed ledger system **14**. Record **40** has a structure that includes an attribute type, a hashed and encrypted value of the attribute, an attester's digital signature of the hashed and encrypted value and the attester's address. An exemplary record format is set out in table below.

User Attribute	Hashed and Encrypted Value	Attester Signature	Attester Address
Attribute	encrypt(attribute)	Signature of encrypt (value)	Address

An exemplary set of records is set out in table below. A set **42** of such records **40** can correspond to a user's profile. This set **42** (or profile) is added to with new records as new attributes of the user are added to the distributed ledger system **14**.

User Attribute	Hashed and Encrypted Value	Attester Signature	Attester Address
Citizenship	encrypt(USA)	Signature of encrypt (USA)	attst@cadmv.com
Current Age	encrypt(age)	Signature of encrypt (age)	attst@cadmv.com
Home Address	encrypt(address)	Signature of encrypt(address)	attst@cadmv.com
Height	encrypt(height)	Signature of encrypt (height)	attst@cadmv.com
Access credentials	encrypt (credentials)	Signature of encrypt(credentials)	secure@serv.com
*	*	*	*
*	*	*	*
*	*	*	*

One can readily observe that what is stored in the distributed ledger system **14** is information about a user's attribute, a hash of that attribute, information about an attester to the attribute, which information is attester signature system, and attester address. The attester when contacted can attest to the requested information being valid. For example, given a user's birth certificate that is issued by a state governmental agency that state governmental agency converts the birth certificate to a digital file of the document, and that digitized file of the document is hashed to provide a hash of the digitized birth certificate document. Rather than the document itself being stored (or the digitized document being stored, what is stored is the hash of the digitized birth certificate document, that is stored in a user's profile in the distributed ledger **14**.

Within a domain, distributed ledgers exchange information to maintain identical ledgers, with any suitable so called sequential transaction database technology of which "Blockchain" technology is but one example. However, unlike some electronic currency based technologies, e.g., bitcoin, where the Blockchain is designed so that no entity controls the Blockchain in some examples disclosed herein using the techniques disclosed herein the transaction database technology actually exchanges information within a domain and because such domains could be private transaction databases, each entity or industry could structure the transaction database as different private transaction databases.

Referring now to FIG. **6**, the broker system **16** is shown. The broker system **16** includes a computer system and executes software that handshakes between the user system **12** and the vetting agent or attester. Rather, than the user device **12***a* accessing the distributed ledger **14**, all requests for transactions between the user device and the requesting device occur through the broker system **16**. For some transactions, the broker system **16** accesses the distributed ledger system **16**, whereas in other transactions the requesting system **18** accesses the distributed ledger system **16**.

As shown in FIG. **6**, the broker system **16** can be a compilation of many such broker systems **16***a*-**16***n*. Each of the broker systems **16***a*-**16***n* can comprise computer systems and associated distributed databases. The broker systems **16***a*-**16***n* are distributed over a network of servers that act together to manage the distributed ledger **14**. All attribute hashed values, attester information, etc. are stored in the distributed ledger **14** and as the flow diagram below will show the broker systems **16***a-n* are configured to access the distributed ledger **14** to obtain and validate such information. Also shown in FIG. **6**, are the encryption and decryption (E/D) of data flows that take place between the broker systems **16***a-n* and wallets **13***a*.

Note that in the context of a private distributed ledger environment, for an enterprise, it may be desirable to not have a query sent to the attester database for each transaction. Rather, a business rule could be established that once a validation event has occurred, then it is good for a period of time, until the attester database is updated etc., so as to reduce latency.

Referring now to FIG. **7**, the wallet **13***a* is shown. The wallet **13***a* includes a file **52** structure and wallet management software **54** that are stored on a user device **12***a* (FIG. **1**). In addition to the software comprising management modules **54***a* that handle request and access to the file structure, as well as receiving user authorizations, etc., the software also includes communication modules **54***b* that exchange information between the wallet and requestor systems, and between the wallet and the broker system **16** (when used) and that receives requests for information that result in messages being displayed on the user device **12***a*.

The wallet **13***a* stores information for handling a third party request for data directly from a user that transmits that information directly from the wallet **13***a* to the third party system **18** in a secure manner. The wallet **13***a* may take several form factors—a physical ID Wallet such as a credit card, smart wearable etc. or it may only need to be the software payload that a system pushes out to a commercially acceptable mobile device such as a smartphone. In some implementations, the wallet needs to be in communication with a device that can perform calculations/determinations, as will be discussed below.

The wallet **13***a* has the management module **54***a* that handles third party requests for information and/or attributes and the communication module **54***b* that interfaces with the broker system **16**. The wallet **13***a* includes a module **54***c* that allows a user to view the request and either approve, all or part of none of the request. Upon approval (partial or all) of the request, the wallet **13***a* encrypts via encryption module **55** the requested information using a public key infrastructure (PKI) where a public key of the third party is used along with one the private keys associated with the wallet **13***a* to encrypt the data. The encrypted data can either be sent to the user's broker system **16** or the wallet **13***a* can look up the direct address of the third party system **18** and send the encrypted data directly to the third party system **18**, depending on the implementation of the system **10**.

As known, a public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. PKI is required for activities where simple passwords are an inadequate authentication method. In cryptography, PKI binds public keys with respective user identities by means of a certificate authority (CA) within a CA domain. The user identity is unique within each CA domain.

Referring now to FIG. **8**, a diagram of a process **60** and flow for the process **60** where the system **18***a* requests information from the user system **12***a*. In this case, the broker system **16** provides an asynchronous transfer between the user device **12***a* and the third party device **18**. The third party device **18** sends a message request **61***a* to the distributed ledger **14** for the user's broker system. In general, there can be many such broker systems associated with many users. The third party device **18** receives **61***b* a message that includes an address of the user's determined broker, as received from the distributed ledger. (In the following figures, as needed, double arrowed lines and reference characters on tips of such arrows are used to denote paired messages, such as sending and receiving messages.) In other implementations, the address lookup can also go through the exchange network.

In an implementation that uses a broker, the third party device **18** (system discussed below) sends **62** a message to the user's determined broker **16**, which message includes a request to access data on the user's wallet **13***a*. The request for data is sent **64** from the broker system **16**. A "score" is calculated for determining the validity of the data (rather than being a measure of the secure transmission of the data). A scoring algorithm can be based on the number and types of attesters, etc., to the user's wallet **13***a* on device **12***a*. Various algorithms can be used such as one that weights types of attesters and number of attesters and normalized these to a standard. Thus, a score generated with a large number of highly trusted attesters would be higher than a score generated with a large number of attesters having a low level of trust. An alternative to this type of score is an attester score based on the type of attester and how trustworthy the attester is and has been. For example, see the following table.

Score	Number of attesters of high trust	Number of attesters of moderate trust	Number of attesters of low trust
0-10	0	0	No more than X
11-20	0	0	Greater than X less than Y
21-40	0	At least M	
*	*	*	*
*	*	*	*
*	*	*	*
91-100	At least Z		

One algorithm, as in the table above, is a mapping scheme that maps a score range (or values) to various slots based on empirically determined number of attesters (M, X, Y, Z) and empirically determined trust levels (high, moderate, low). This could be an example of a score for an item. Thus, with an item could be stored the number of and types of attesters of various categories (three of which, low, moderate and high trust levels being shown) or the score range or value.

Other scoring algorithms such as weighted algorithms could be used, such as one of the form:

$$\text{Score}=((H*W_h+M*W_m+L*W_h)/\text{total})/\text{Normalized}$$

Where H is the total of high trusted attesters
M is the total of moderately trusted attesters
L is the total of low trusted attesters
W_h; W_m; W_h are empirically determined weights, and Normalized is an optional normalization function or value.

The user's wallet **13***a* (or other application or user via a physical action using a user input device) either answers (yes or no) or simply ignores the message. When the answer is yes, the user's wallet **13***a* (or other application) encrypts the data using an asymmetric encryption algorithm that uses the requestor's public key. The encrypted data is sent **66** from the user's wallet **13***a* to the broker system **16** so that only the two endpoints (user's wallet **13***a* and the third party system **18**) can read the actual data. At the broker **16** system, upon reception of the encrypted data from the user's wallet **18***a*, the broker system **16** sends the data to the third party system **18**.

In another implementation, the data would be sent directly to the requestor's wallet without the broker system **16**. This implementation can be especially used with the processes discussed below. In the processes below, this direct approach is used in the explanations of those processes.

Referring now to FIG. **9**, another process **70** is shown in which there is a required validation of PII data through a distributed public ledger **14***a*. The distributed ledgers can be public, meaning that anyone can place and/or access data in the ledger or private, meaning that only authorized individuals and entities can place and/or access the private type of ledger. Thus, generically, such distributed ledgers **14** can be public or private depending on various considerations. In either instance, the ledger **14** contains the information needed to validate the brokered information. The third party system **18** sends **72** a lookup request to the distributed ledger **14***a* for a particular user's attribute.

In FIG. **9**, the broker **16** and wallet **13***a* and user device **12***a* are not directly involved, but are shown. The lookup request is actually for a hash of the desired user's attribute. The distributed public ledger **14***a* receives the request and accesses the hash of the particular user's attribute and returns **72***b* that hash to the third party system **18**. The third party system **18** sends **74***a* a look up message request for the system that has attested to the hash of the particular user's attribute stored in the distributed public ledger **14***a*. The third party system **18** receives **74***b* the identity of the system that performed the attestation to the hash of the particular user's attribute, and makes an independent decision **75** on the validity of the hash of the particular user's attribute. For cases where privacy of the data is a concern this case assumes that the third party system has the user's public key, as the attribute data is encrypted. For other types of data where privacy of the data is not a concern, the attribute need not be encrypted.

Note, in addition to returning the attester information, the system could return the attester score of that attester having the highest score. The score could be calculated by the distributed ledger **14**, but may be more appropriately calculated by the broker system.

Referring now to FIG. **10**, another process **80** is shown in which there is required validation of data through a private distributed ledger **14***b*. The third party system **18** sends **82***a* a message to a broker directory system **15** to locate the user's (potential driver's) broker system. The broker directory system **17** determines the user's broker system and sends **82***b* a message to the third party system **18**, which includes the identity of the user's broker system. The third party system **18** sends **84** a message to the determined broker system **16**, which is a request to the user's broker system **16** to validate data and return score data. There are many algorithms that could be used for scoring. For example, a simple algorithm may assign a score to an attester as high, when the attester is a governmental agency and may score an attester as lower when the attester is a personal contact. The user's broker system **16** validates data by sending **86***a* a message to the distributed ledger **14***b* for the data and the score (of the data or the attester). The broker receives **86***b* from the distributed ledger **14***b* a message including the data and the score(s). The user's broker system **16** returns **88** the score(s) and status back to the third party system **18**.

One approach for a private enterprise would be for an enterprise to define business rules that govern source attester scores. The rules could be absolutes. Alternatively, over time the system that determines the score builds "a transactional footprint" for transactions, which is based on physical access points, logical access points, time of day, duration of use, etc. used with a transaction record. Initial algorithms are determined at the initial deployment, and then are refined based upon a regression pattern(s) that emerges.

Optionally, the third party system **18** requests **92***a* a lookup of the broker/owner for the party that verified the data. The third party receives **92***b* the address of the broker/owner that verifies the data. The broker/owner system that verifies the data signs the data with its digital signature. The broker/owner system sends **94***a* a message to the verifying broker/owner to verify a signature of the signed data. Upon receiving **94***b* a verification from the verifying broker/owner system, the third party system has verification of the data without actually having accessed the data. Optionally, the user can share **96** the data to be validated with the third party directly from the user's wallet.

Another process (not shown) can be used in which a third party requests validation of an attribute without actually disclosing the attribute. In this process the wallet **13***a* does not send a hash of the attribute, but allows a third party to request the verification of the attribute from the exchange. The rule is submitted to the exchange of the user (i.e. the request to validate if the user has a valid driver license and/or an absence of a criminal record or outstanding moving violations). The user would authorize the exchange for this rule to be processed. A trusted party attests to the valid driver license and/or the absence of a criminal record or outstanding moving violations.

Credential-Based Registration System

Described below are aspects of a mobile credential. The mobile credential is stored in a user's wallet **13***a* and is identified as authentic by use of the distributed ledger **14**. The distributed ledger **14** is used to supply secure credentials to the user's wallet **13***a* all of which have been validated by the distributed ledger **14**. The mobile credential is used to produce an access token that has a finite lifespan that is determined according to the estimate provided by the system of FIG. **4**, and which can be adjusted. With the processes described below, the reader system can verify the access token as authentic and being from the user, and the user's wallet **13***a* can verify the vehicle as the vehicle to which the user should exchange credentials.

Referring now to FIG. **11**, a credential-based registration/access system **180** that is a specialization of the system of FIG. **1**, without the use of a broker system, is shown. The credential-based registration/access system **180** (registration/access system **180**) is used for registration of a mobile credential with an access control system (not shown) using registration process **188***a*, the details of which will be discussed below. The registration/access system **180** includes the user device **12***a* having the wallet **13***a*. It is understood that a practical implementation would in general involve many such user devices/wallets of many users. The user device **12***a* and wallet **13***a* will be registered with the access control system and verified for use with the access control system. The registration allows a specific vehicle to be registered by the mobile credential.

The credential-based registration/access system **180** (system **180**) also includes a vehicle system **184** including a vehicle wallet **187** and a vehicle application **188** that together with the user device **12***a* registers and verifies users, e.g., employees of an entity controlling the physical premises or logical structures, by use of the distributed ledger **14** and the distributed network server computers **190**. The user device and the system can be any type of computing system, computing station, computer server, tablet device, etc., that includes Bluetooth® or other near field communication capabilities that can send out a beacon signal, as discussed below. The application **188** causes the system **184** to continually or periodically issue the beacon that is readable by the user device **12***a* to initiate a transaction with the system **184**.

Referring now to FIG. **12**, a credential-based registration process flow **200** for registration of a mobile credential stored on the user device **12***a* (more specifically in the wallet **13***a*) with access control systems is shown. Shown in FIG. **12**, are user device processing (FIG. **12**A), system processing (FIG. **12**B) and distributed system/distributed ledger processing (**12**C). This credential-based registration process flow **200** (registration process **200**) is shown for the user device **12***a*/wallet **13***a*, system **184**/application **188**, and the distributed servers **190** that interact with the distributed ledgers **14**. The registration process **200** allows a user to verify a vehicle. The registration process flow **200** also allows the access control system to verify the identity of the user possessing the mobile credential for permitting registration for access to the vehicle. The described registration process **200** uses the application **188** to register and verify the user.

Referring now to FIG. **12**A, the user device **12***a* portion credential-based registration process flow **200** is shown. The user device **12***a* listens **202** for a beacon from the system. The beacon includes a message to cause the user's device to initiate **204** a transaction with the server to send the user's public key stored in the user's wallet **13***a*. The user's public key can be embedded in a code, such as a "QR"™ code (type of matrix barcode) that is stored in the user's wallet **13***a*. Other approaches could be used.

The user's wallet **13***a* requests **206** from a wallet **187** of the system **184**, e.g., application **188**, an access QR code has embedded therein a vehicle public key. In some implementations, the vehicle public key as well as a vehicle UUID (discussed below) are specific to a single physical vehicle. However, in other implementations, the vehicle public key as well as the vehicle UUID are specific to a plurality of vehicles of a single or related set of services. From the wallet **13***a*, a user profile corresponding the user associated with the device **12***a* is sent **208** to the application **188**. As used herein a UUID is an identifier, e.g., such as a Universally Unique Identifier (UUID) per the UUID identifier standard that uses a 128-bit value.

Referring now also to FIG. **12**B, the application **188** causes the system to continually or periodically issue **222**, a beacon, e.g., an electronic signal that is readable by the user device **12***a*. The application receives **224** the user's public key. A wallet **201** of the application sends **226** a QR code that has a vehicle public key. The application receives **228** the user's profile corresponding the user associated with the device **12***a*. Upon receiving the user profile, the application **188** sends **228** a message to distributed networked servers to search for the user via the distributed ledger **14**. This search would be for the user's PII information.

Upon receipt **230** of a search result, if the user does not exist in the distributed ledger system **14**, then the system will produce **232** a fault message. If the user profile does exist it may be updated **234**, if needed, based on the received profile information. The system sends **236** updated user identity to the distributed ledger **14**, along with the received public key to the distributed ledger system **14** where the profile, public key of the user are stored.

At this juncture, the user has been verified. Thus, upon verification of the user, the vehicle can be assured that it can exchange credentials with the user device **12***a* and wallet **13***a*. The system via the application **188** sends **238** a message to the distributed network servers to obtain the vehicle UUID and the vehicle public key from the distributed ledger **14** and upon receiving the vehicle UUID and vehicle public key, sends **220** the vehicle UUID and the vehicle public key to the wallet **13***a* for verification and storage. The wallet **13***a* receives **210** a message from the system, which contains the vehicle UUID and the vehicle public key. The wallet **13***a* verifies **212** the vehicle public key using similar processes as discussed above. If verified the user device **12***a* and wallet **13***a* can be assured that this is a vehicle for which the user device **12***a* and wallet **13***a* can furnish a mobile credential. When verified the wallet stores **214** the UUID and vehicle public key.

Referring now to FIG. **12**C, the distributed servers receive **252** a message from the system to conduct a search for a profile of the user. The distributed servers access **254** the distributed ledger **14**. The distributed servers determine **256** if a profile exists by searching the distributed ledger system **14** for a profile of the user. The distributed servers send **258** a result of the search, e.g., registered, not registered, expired registration, etc. to the system **18**.

Credential-Based User Access

Credential-based access processing for permitting access using a registered mobile credential stored on the user device **12***a* (more specifically in the wallet **13***a*) to an access control system, uses the user device, access systems and the distributed system/distributed ledger system. Access processing allows a user, e.g., user, to verify a vehicle and vice-versa.

The credential process uses a credential exchange mechanism that allows a user's wallet **13***a* to verify the vehicle, obviating need for a central, certificate issuing authority, by each vehicle having a unique certificate similar to those commonly found today in website certificates. However, in this instance, the company is the issuer of the certificate. This gives the ability to have the credential carrier roles and permissions, conveyed by the reader application exchanging the roles and permissions of a user, without having to go back to a central service. This allows local control (exchange process of certificates). The mobile wallet **13***a* can access permissions from a central facility (one time load) without the local control having to go back to the central facility each time access is attempted.

User access to a vehicle can give door access to the vehicle, if the user has a seal (discussed below) and is scheduled for access to the vehicle (e.g., rental). As used herein, a "seal" is a token that is registered on a user' wallet **13***s* to verify that the user has gone through an initial authentication process. This "seal" would contain a signature from the server **184** that validated the user's wallet under specified conditions (time interval, level, etc.).

The user is registered and when the user shows up at the vehicle, the user will scan an outside reader or the vehicle will sense credentials to gain access. Details of these processes are discussed below.

Digital certificates are issued by a certificate authority or certification authority (CA), i.e., an entity that issues and certifies digital certificates, which certification is used to verify the ownership of a public key by the named entity associated with the certificate. The certification enables others that rely upon signatures or assertions made about the private key as corresponding to the certified public key. In this model of trust relationships, a CA could be a third party or in some implementations could be the entity itself rather than a trusted third party—trusted both by the owner of the certificate and by parties that would be relying on the certificate. Public-key infrastructure (PKI) schemes feature certifying authorities.

Described is a vehicle application **188** to access and verify users or other service providers. The user's device **12***a* listens for a beacon. The vehicle broadcasts a beacon (ID) that the user's device, e.g., smartphone receives and, which the mobile wallet **13***a* detects. The user device **12***a* connects to the vehicle computer, and the wallet **13***a* via the device **12***a* requests that the computer provide its credentials to the user device **12***a*. The beacon includes a message to cause the user's device **12***a* to initiate **604** a transaction with the application on the computer. The user's wallet **13***a* requests **606** a vehicle certificate, OCSP and vehicle UUID (discussed below).

The user's device **12***a* verifies **608** the credentials sent to the wallet **13***a* from the vehicle wallet **201**, e.g., the vehicle certificate, the OCSP and the vehicle UUID. If valid, then the system will provide its UUID, the vehicle certificate (public key for the vehicle) and company certificate (e.g., public key of the rental company). The wallet **13***a* verifies if, the wallet **13***a*, is paired with the rental company.

Since the mobile wallet knows the company's public key, the mobile wallet can trust that any packets signed by the company are valid and can be trusted. When the mobile wallet **13***a* accesses a vehicle, the vehicle provides its specific public key to the mobile device **12***a* (wallet **13***a*). Authenticity of the vehicle is determined by the wallet **13***a* through verification **608** of the vehicle's certificate. The verification process has the wallet **13***a* determine whether the vehicle certificate was signed by the company. If the certificate was signed by the company, then the wallet **13***a* verifies that the vehicle certificate and the signature match because the wallet has the company's public key and the wallet can verify the signature. If the signature is valid, then the wallet **13***a* knows that the vehicle certificate is authentic.

Although the certificate is authentic the wallet needs to verify that the certificate has not been revoked. The wallet can do this verification a number of ways.

Upon, the user's wallet **13***a* verifying the vehicle credentials, e.g., vehicle certificate, a revocation status and vehicle UUID, the user's wallet sends **610** a JWT message to the door kiosk app. The JWT message follows the so called JSON Web Token (JWT) format that is a JSON-based open standard (RFC 7519) for producing tokens that assert some number of "claims." The generated tokens, as above, are signed by the token producer's private key, so that door app in possession of the producer's public key is able to verify that the token is legitimate. An exemplary JWT message is

JWT Format

Claims	
iss	Issuer. The UUID of the Mobile Wallet
aud	The UUID of the Reader being accessed
exp	Expiration time of the token. Set to 30 seconds
jti	Unique token id. Server will track IDs over the expiration time period to ensure not duplicate JWT calls are made
iat	Time the token was issued/created

The JWT contains the "iss" attribute which is a unique ID for the wallet. This unique ID is used by the reader or other system to obtain the stored public key and the JWT can be verified. If the token is not valid then an error response is sent to the wallet and access is not provided. The JWT has an "aud" attribute that identifies the destination of the token (i.e., the reader UUID). The JWT also includes an "exp" attribute that sets the expiration time of the token, and a "jti" attribute, i.e., and ID that can be used by the Reader or which can be used by an upstream system to ensure that the token can be used only once during the validity time (i.e., replays would be prevented). The "iat" attribute indicates the time that the JWT was issued.

Thus, the application **188** can send to the user device containing the wallet **13***a* a verified access or access error depending on the outcome of the process. All exchanges are logged in the distributed ledger for audit tracking, etc.

The JWT can also contain access policies that the reader can implement locally. For example, the JWT could contain roles that the wallet belongs to and those roles can be used by the reader to determine if the access should be provided or not with all decisions being made by the reader unit. This provides reduced latency in comparison with a centralized system approach where decisions based on roles, etc. are centrally made. The roles and access policies would be part of a JWT payload. A requirement would thus be that those roles and policies would need to be signed by the company and preferably would have an expiration date.

The reader will trust those policies if they meet the validation criteria which is composed of the follow types of checks:

The policies contain the wallet ID

The policies are signed by the Company

The policies are not expired

The specifics of the encoding of the JWT payload have not been provided. However, the payload could be a binary payload inside of the JWT, an encoded attribute, or could be a second JWT produced by the company that the mobile wallet provides in addition to its own JWT, i.e., the company provided JWT for access. This second JWT produced by the company would contains the access policies, wallet id, and expiration time, would be signed by the company and the "iss" of the company.

Referring now to FIG. **13**A, the user device **12***a* portion **700***a* of the credential-based access process **700** is shown. The user device **12***a* listens **702** for a beacon from a reader. The reader broadcasts a beacon (ID) that the smartphone receives and, which the mobile wallet detects. The user device **12***a* connects to the reader, and the wallet **13***a* via the device **12***a* requests that the reader provide its credentials to the user's device **12***a*. The beacon includes a message to cause the user's device **12***a* to initiate **704** a transaction with the reader to connect with the application on the reader. The user's wallet **13***a* requests **706** from a wallet **701** in the reader, e.g., application **188**, a vehicle certificate, OCSP and vehicle UUID (discussed below).

The user's device **12***a* verifies **708** the credentials sent to the wallet **13***a* from the wallet **701** of the system **184**, e.g., the vehicle certificate, the OCSP and the vehicle UUID. If the reader is valid, then the reader will provide its vehicle UUID, the vehicle certificate (public key for the vehicle) as well as the company UUID and company certificate (public key of the company). The wallet **13***a* verifies if, the wallet **13***a*, is paired with the correct vehicle.

Other approaches include the beacon ID being that of the company UUID and if the wallet **13***a* is paired with that company, the wallet **13***a* (via the device **12***a*) then connects to the system and requests details. The wallet **13***a* via the device **12***a* either connects and determines if the beacon is from a valid system or the beacon ID itself is formatted such that beacon from a valid system informs the wallet **13***a* that the beacon is from the reader and the wallet verifies the specifics by connecting to the reader.

The user's wallet connects to the application once the beacon is detected. The application has the vehicle certificate, the vehicle UUID, and a revocation status, e.g., such as via the "Online Certificate Status Protocol" (OCSP) as discussed above. Other approaches could be used.

Since the mobile wallet knows the company's public key, the mobile wallet can trust that any packets signed by the company are valid and can be trusted. When the mobile wallet **13***a* accesses the reader, the reader provides its vehicle specific public key to the mobile device **12***a* (wallet **13***a*). The mobile wallet **13***a* does not know if this vehicle is authentic and part of the company that the wallet **13***a* holds a mobile credential for, and thus before the wallet **13***a* exchanges its credentials, the wallet **13***a* needs to verify for certain that the reader is authentic.

Authenticity of the reader is determined by the wallet **13***a* through verification **708** of the vehicle's certificate. The verification process has the wallet **13***a* determine whether the vehicle certificate was signed by the company. If the certificate was signed by the company, then the wallet **13***a* verifies that the vehicle certificate and the signature match because the wallet has the company's public key and the wallet can verify the signature. If the signature is valid, then the wallet **13***a* knows that the vehicle certificate is authentic.

Although the certificate is authentic the wallet needs to verify that the certificate has not been revoked. The wallet can do this verification a number of ways as discussed above, e.g. directly through an OCSP request or with an OCSP response (i.e. OCSP stapling), as discussed above, or CRL.

Upon, the user's wallet **13***a* verifying the vehicle credentials, e.g., vehicle certificate, a revocation status and vehicle UUID, the user's wallet sends **710** a JWT message to the reader. The JWT message follows the so called JSON Web Token (JWT) format discussed above. The generated tokens, as above, are signed by the token producer's private key, so that door kiosk app in possession of the producer's public key is able to verify that the token is legitimate. The claims are used to pass identity of authenticated users between an identity provider and a service provider. The tokens can be authenticated and encrypted. Upon verification of the JWT message by the servers, the servers cause the reader to send an access status message that is received **712** by the wallet **13***a*, allowing or denying access.

Referring now also to FIG. **13**B, the application **188** processing **700***b* causes the system reader to continually or periodically issue **722**, the beacon that is readable by the user device **12***a* and which causes the user device to request **724** a connection to the reader. As mentioned above, the user device **12***a* upon connecting to the reader has the reader provide **726** its credentials to the user's device **12***a* (wallet **13***a*). If the verification by the wallet was successful, the wallet sends the JWT message, and upon receipt **728** of the JWT message by the reader, the JWT is sent **730** to the distributed network to a server that is used to verify the JWT token. Upon verification of the JWT message by the servers, the servers send the reader an access status message that is received **732** and is sent **734** to the wallet **13***a* allowing or denying access to the vehicle.

Referring now also to FIG. **13**C, the distributed servers/distributed ledger processing **700***c* is shown. The JWT is received **742** by the distributed servers and is verified **744**. If the JWT is not verified, an error is raised **748** (see below). If the JWT is verified, **746** the user is granted access **750**, and an access control system grants the access and sends signal to unlock a door, etc. In addition, whether the JWT is verified or not verified, a corresponding entry record of either an access entry or an access denied entry is produced **752** as an access log that is stored **754** and maintained in the distributed ledger system.

All exchanges are logged in the distributed ledger for audit tracking, etc. Records are added to the distributed ledger as transactions and include a hashed record of the transaction, what was exchanged, the signatures of the parties, and may include additional detailed information depending on the type of distributed ledger used. The information stored for audit can include the date and time that the mobile wallet sent a JWT, the JWT parameters, and the access status or error conditions.

Referring now to FIG. **14**, components of system/devices are shown. Memory stores program instructions and data used by the processor. The memory may be a suitable combination of random access memory and read-only memory, and may host suitable program instructions (e.g. firmware or operating software), and configuration and operating data and may be organized as a file system or otherwise. The program instructions stored in the memory may further store software components allowing network communications and establishment of connections to the data network. The software components may, for example, include an internet protocol (IP) stack, as well as driver components for the various interfaces. Other software components suitable for establishing a connection and communicating across network will be apparent to those of ordinary skill.

Servers are associated with an IP address and port(s) by which it communicates with user devices. The server address may be static, and thus always identify a particular one of monitoring server to the intrusion detection panels. Alternatively, dynamic addresses could be used, and associated with static domain names, resolved through a domain name service. The network interface card interfaces with the network to receive incoming signals, and may for example take the form of an Ethernet network interface card (NIC). The servers may be computers, thin-clients, or the like, to which received data representative of an alarm event is passed for handling by human operators. The monitoring station may further include, or have access to, a subscriber database that includes a database under control of a database engine. The database may contain entries corresponding to the various subscriber devices/processes to panels like the panel that are serviced by the monitoring station.

All or part of the processes described herein and their various modifications (hereinafter referred to as "the processes") can be implemented, at least in part, via a computer program product, i.e., a computer program tangibly embodied in one or more tangible, physical hardware storage devices that are computer and/or machine-readable storage devices for execution by, or to control the operation of, data processing apparatus, e.g., a programmable processor, a computer, or multiple computers. A computer program can be written in any form of programming language, including compiled or interpreted languages, and it can be deployed in any form, including as a stand-alone program or as a module, component, subroutine, or other unit suitable for use in a computing environment. A computer program can be deployed to be executed on one computer or on multiple computers at one site or distributed across multiple sites and interconnected by a network.

Processors suitable for the execution of a computer program include, by way of example, both general and special purpose microprocessors, and any one or more processors of any kind of digital computer. Generally, a processor will receive instructions and data from a read-only storage area or a random access storage area or both. Elements of a computer (including a server) include one or more processors for executing instructions and one or more storage area devices for storing instructions and data. Generally, a computer will also include, or be operatively coupled to receive data from, or transfer data to, or both, one or more machine-readable storage media, such as mass storage devices for storing data, e.g., magnetic, magneto-optical disks, or optical disks.

Computer program products are stored in a tangible form on non-transitory computer readable media and non-transitory physical hardware storage devices that are suitable for embodying computer program instructions and data. These include all forms of non-volatile storage, including by way of example, semiconductor storage area devices, e.g., EPROM, EEPROM, and flash storage area devices; magnetic disks, e.g., internal hard disks or removable disks; magneto-optical disks; and CD-ROM and DVD-ROM disks and volatile computer memory, e.g., RAM such as static and dynamic RAM, as well as erasable memory, e.g., flash memory and other non-transitory devices.

In addition, the logic flows depicted in the figures do not require the particular order shown, or sequential order, to achieve desirable results. In addition, other actions may be provided, or actions may be eliminated, from the described flows, and other components may be added to, or removed from, the described systems. Likewise, actions depicted in the figures may be performed by different entities or consolidated.

Elements of different embodiments described herein may be combined to form other embodiments not specifically set forth above. Elements may be left out of the processes, computer programs, Web pages, etc. described herein without adversely affecting their operation. Furthermore, various separate elements may be combined into one or more individual elements to perform the functions described herein.

Other implementations not specifically described herein are also within the scope of the following claims.

What is claimed is:

1. A method of monitoring use of an asset comprises:

transmitting, to a user portable electronic device by an asset access application executable in a computing system in the asset, credentials associated with the asset, wherein the user portable electronic device authenticates the asset based on the credentials;

receiving, from the user portable electronic device and in response to the user portable electronic device authenticating the asset, an electronic representation of a user's identity and an electronic representation of authenticating items, by the asset access application executable in the computing system in the asset, wherein the electronic representation of a user's identity and the electronic representation of authenticating items are stored in a distributed ledger comprising distributed databases controlled by a distributed database management system, the distributed ledger configured to identify changes in the electronic representation of the user's identity and the electronic representation of authenticating items and replicate the changes across the distributed databases, wherein duplication software identifies a first database of the distributed databases as a master database and duplicates the master database across other databases such that the contents of the distributed databases are the same;

sending by the computing system to an identity and access management system the received electronic representation of the user's identity and the electronic representation of authenticating items;

receiving by the computing system from the identity and access management system credentials that validate the electronic representation of the user's identity and the electronic representation of authenticating items;

enabling by the computing system access to the asset when the computing system receives the credentials that validated the user's identity and the electronic representation of authenticating items; and

unlocking and preparing the asset to be operated by the user.

2. The method of claim **1** wherein the asset is a physical asset and receiving the electronic representation of the user's identity, comprises:

receiving a representation of personally identifiable information from a user wallet in the user portable electronic device.

3. The method of claim **2** further comprising:

sending by the computing system a request to the user portable electronic device for presentation of specific types of personally identifiable information from the user wallet.

4. The method of claim **2** wherein the requested information includes one or more of birth date, driver license number, home address, social security number.

5. The method of claim **2** wherein the requested information is represented as a verification from the identity and access management system of the representation of the personally identifiable information from the user.

6. The method of claim **2** wherein the identity and access management system, comprises a distributed ledger system and a broker system with the broker system in communication with the computing system and an electronic identity wallet carried on a user device.

7. The method of claim **2** wherein the identity and access management system, comprises a distributed ledger system in communication with the computing system and an electronic identity wallet carried on a user device.

8. The method of claim **2** wherein the credentials received from the identity and access management system are encrypted.

9. The method of claim **2** wherein the vehicle is equipped with one or more sensors and the computing system receives sensor data and processes the sensor data to determine a status of the user, and the method comprises enabling by the system the starting of the vehicle when the system determines the user has a non-impaired status.

10. The method of claim **2** wherein the computing system includes a processor and memory.

11. The method of claim **2** wherein the computing system is a computing system that controls a battery system in the vehicle and which computing system includes a processor and memory to execute an application to receive a validation of the user's identity and the user authorization to drive the vehicle before applying battery power to the remainder of the vehicle.

12. A system for monitoring use of a vehicle comprises:

a computing system including processor and memory and storing computing instructions to cause the computing system to:

transmit, to a user portable electronic device, credentials associated with the vehicle, wherein the user portable electronic device authenticates the vehicle based on the credentials;

receive, from the user portable electronic device and in response to the user portable electronic device authenticating the vehicle, an electronic representation of a user's identity and an electronic representation of authenticating items, by a vehicle access application executable in a computing system in the vehicle, wherein the electronic representation of a user's identity and the electronic representation of authenticating items are stored in a distributed ledger comprising distributed databases controlled by a distributed database management system, the distributed ledger configured to identify changes in the electronic representation of the user's identity and the electronic representation of authenticating items and replicate the changes across the distributed databases, wherein duplication software identifies a first database of the distributed databases as a master database and duplicates the master database across other databases such that the contents of the distributed databases are the same;

send to an identity and access management system the received electronic representation of the user's identity and electronic representation of authenticating items;

receive from the identity and access management system credentials that validate the electronic representation of the user's identity and the electronic representation of authenticating items; and

enable starting of the vehicle when the computing system receives the credentials that validated the user's identity.

13. The system of claim **12** wherein the computing system is configured to send a request to the portable electronic device for presentation of specific types of personally identifiable information.

14. The system of claim **13** wherein the electronic representation of a user's identity includes one or more of birth date, driver license number, home address, social security number.

15. The system of claim **12** wherein the electronic representation of a user's identity is encrypted.

16. The system of claim **12** wherein the computing system is a computing system that controls a battery system within the vehicle.

17. The system of claim **12** wherein the vehicle is equipped with one or more sensors and the computing system receives sensor data and processes the sensor data to determine a status of a user and enable the starting of the vehicle when the system determines the user has a non-impaired status.

18. A computer program product stored on a non-transitory computer readable medium for monitoring use of a vehicle comprises instructions to cause a computing device to:

transmit, to a user portable electronic device, credentials associated with the vehicle, wherein the user portable electronic device authenticates the vehicle based on the credentials;

receive, from the user portable electronic device and in response to the user portable electronic device authenticating the vehicle, an electronic representation of a user's identity and an electronic representation of authenticating items, by a vehicle access application executable in a computing system in the vehicle, wherein the electronic representation of a user's identity and the electronic representation of authenticating items are stored in a distributed ledger comprising distributed databases controlled by a distributed database management system, the distributed ledger configured to identify changes in the electronic representation of the user's identity and the electronic representation of authenticating items and replicate the changes across the distributed databases, wherein duplication software identifies a first database of the distributed databases as a master database and duplicates the master database across other databases such that the contents of the distributed databases are the same;

send to an identity and access management system the received electronic representation of the user's identity and the electronic representation of authenticating items;

receive from the identity and access management system credentials that validate the electronic representation of the user's identity and the electronic representation of authenticating items; and

enable starting of the vehicle when the computing system receives the credentials that validated the user's identity.

19. The computer program product of claim **18** wherein the computing system is configured to send a request to the portable electronic device for presentation of specific types of personally identifiable information.

20. The computer program product of claim **19** wherein the electronic representation of a user's identity includes one or more of birth date, driver license number, home address, social security number.

* * * * *