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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 October 2021 (21.10.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/211983 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *H04L 9/32* (2006.01)
H04L 29/06 (2006.01) *H04W 12/08* (2021.01)

(21) International Application Number: PCT/US2021/027706

(22) International Filing Date: 16 April 2021 (16.04.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
63/011,185 16 April 2020 (16.04.2020) US

(71) Applicant: MASTERCARD INTERNATIONAL INCORPORATED [US/US]; 2000 Purchase Street, Purchase, NY 10577 (US).

(72) Inventors: PRASZCZALEK, Przemek; 19107 Hartline Green Drive, Cypress, TX 77433 (US). NARAYANSWAMY, Raman; 3 Sandstone Drive, Nashua, NH 03063 (US).

(74) Agent: DOBBYN, Colm, J.; Mastercard International Incorporated, 2000 Purchase Street, Purchase, NY 10577 (US).

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

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) Title: SYSTEMS, METHODS, AND NON-TRANSITORY COMPUTER-READABLE MEDIA FOR SECURE BIOMETRICALLY-ENHANCED DATA EXCHANGES AND DATA STORAGE

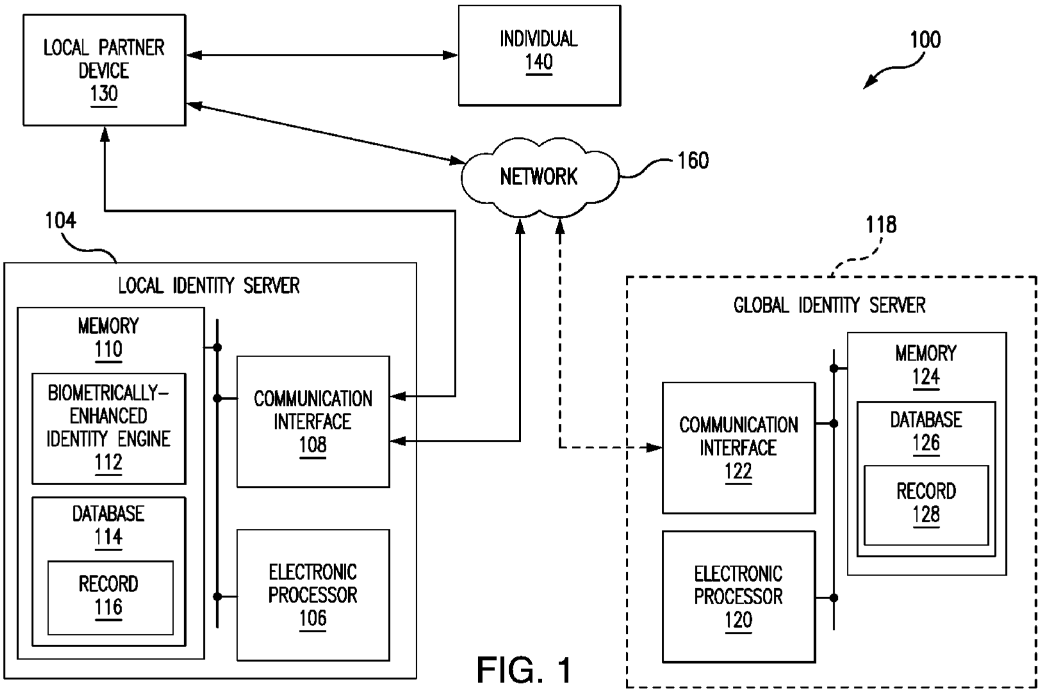


FIG. 1

(57) Abstract: A privacy-enhancing system, method, and non-transitory computer-readable medium for securely identifying or verifying an individual over time without retaining sensitive biometric data (e.g., biometric images or biometric templates) for the purpose of securely storing data regarding the individual.

[Continued on next page]

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

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

SYSTEMS, METHODS, AND NON-TRANSITORY COMPUTER-READABLE MEDIA FOR SECURE BIOMETRICALLY-ENHANCED DATA EXCHANGES AND DATA STORAGE

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Application No. 63/011,185, filed on April 16, 2020, the entire content of which is hereby incorporated by reference.

FIELD OF THE INVENTION

The present disclosure relates generally to secure data exchanges or data storage. More specifically, the present disclosure relates privacy-enhancing systems, methods, and non-transitory computer-readable media with biometrically-enhanced data exchanges or storage.

BACKGROUND

A digital identification and personal data exchange improve privacy and security of individual's data which is accesses, shared, and exchanged between various individuals and entities. In particular, a digital identification and personal data exchange will help prevent unauthorized actors from assuming identities or gaining access to personal data of individuals. Use of digital identity service and data exchange service will also help facilitate new, innovative approaches to digital payments, commerce and financial inclusion.

The digital verification and identification as described herein is referred to as “Inclusive Verification of Identity.” The following are aspects of a successful implementation of Inclusive Verification of Identity and Personal Data Exchange.

SUMMARY

A partner-specific identification Digital identification and personal data exchange will help in addressing the aftermath of the COVID-19 pandemic. In particular, a digital identification and personal data exchange will help prevent or counter nefarious actors from assuming identities or gaining access to personal data of victims of the COVID-19 pandemic. Use of digital identity service and data exchange service will also help facilitate new, innovative approaches to digital payments, commerce and financial inclusion.

One embodiment of the present disclosure includes a system for securely storing information of an individual. The system includes a local partner device that includes a first electronic processor, a first communication interface, and a first memory. The first electronic processor is configured to receive biometrics and registration information of an individual, generate, with a tokenization algorithm, a first biometric token based on the biometrics that are received, and create a data account associated with the individual in the first memory, the data account including the registration information and the first biometric token. The first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual with the tokenization algorithm.

Another embodiment of the present disclosure includes a method for securely storing information of an individual. The method includes receiving, with a local partner device, biometrics and registration information of an individual. The method includes generating, with the local partner device and a tokenization algorithm, a first biometric token based on the biometrics that are received. The method also includes creating, with the local partner device, a data account associated with the individual in a memory, the data account including the registration information and the first biometric token. The first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual with the tokenization algorithm.

Yet another embodiment of the present disclosure includes a non-transitory computer-readable medium comprising instructions that, when executed by an electronic processor, causes the electronic processor to perform a set of operations. The set of operations includes receiving, with a local partner device, biometrics and registration information of an individual. The set of operations includes generating, with the local partner device and a tokenization algorithm, a first biometric token based on the biometrics that are received. The set of operation also includes creating, with the local partner device, a data account associated with the individual in a memory, the data account including the registration information and the first biometric token. The first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual with the tokenization algorithm.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 is a block diagram illustrating an example system 100 for securely identifying and verifying an individual in a biometrically-enhanced data exchange or data storage.

FIG. 2 is a block diagram illustrating a more detailed example of the system of FIG. 1 for securely identifying an individual.

FIG. 3 is a flow diagram illustrating an example operation of the system of FIG. 1 for registering/enrolling the individual in an identity network services platform.

FIG. 4 is a diagram illustrating a comparison between conventional verification of presence and inclusive verification of presence.

FIG. 5 is a diagram illustrating a comparison between conventional verification of presence with a financial product and inclusive verification of presence with a financial product.

FIG. 6 is a flow diagram illustrating an example for issuing a digital identity credential of a registered individual with the system of FIG. 1.

FIG. 7 is flow diagram illustrating example for registering and accessing decentralized points of service with the system of FIG. 1.

FIG. 8 is flow diagram illustrating example for registering and accessing healthcare with the system of FIG. 1.

FIG. 9 is flow diagram illustrating example for registering for healthcare with the system of FIG. 1.

FIG. 10 is flow diagram illustrating examples for biometrically-enhancing data exchange and records matching with the system of FIG. 1.

FIG. 11 is flow diagram illustrating examples for paying for items using biometrics versus smartphone with the system of FIG. 1.

FIG. 12 is flow diagram illustrating examples for payment with secure biometrics and one-time credentials with the system of FIG. 1.

FIG. 13 is flow diagram illustrating examples for smart checkout with the system of FIG. 1.

FIG. 14 is flow diagram illustrating examples for checking out using an application versus biometrics only with the system of FIG. 1.

FIG. 15 is flow diagram illustrating an example of creating or updating user-centric data pods with the system of FIG. 1.

FIG. 16 is flow diagram illustrating an example authorizing data sharing from the digital data pod of FIG. 15 using a consent management module.

FIG. 17 is flow diagram illustrating an example authorizing time-limited data sharing from the digital data pod of FIG. 15 using a consent management module.

FIG. 18 is flow diagram illustrating an example authorizing time-limited data sharing from the digital data pod of FIG. 15 using a consent management module.

FIG. 19 is flow diagram illustrating an example of an individual registering with a partner and establishing a data pod with the system of FIG. 1.

FIG. 20 is flow diagram illustrating an example of an individual registering with another partner and updating a data pod with the system of FIG. 1.

FIG. 21 is flow diagram illustrating an example of an individual accessing a data pod at a point of service with the system of FIG. 1.

FIG. 22 is flow diagram illustrating an example process for securely storing information of an individual.

DETAILED DESCRIPTION OF THE EMBODIMENTS

FIG. 1 is a block diagram illustrating an example system 100 for securely identifying and verifying an individual in a biometrically-enhanced data exchange or data storage, in accordance with various aspects of the present disclosure. In the example of FIG. 1, the system 100 includes a local identity server 104, an optional global identity server 118, a local partner device 130, an individual 140, and a network 160.

The local identity server 104 and the optional global identity server 118 may be owned by, or operated by or on behalf of, an administrator. The optional global identity server 118 may also be implemented by one or more networked computer servers.

The local identity server 104 includes an electronic processor 106, a communication interface 108, and a memory 110. The electronic processor 106 is communicatively coupled to the communication interface 108 and the memory 110. The electronic processor 106 is a microprocessor or another suitable processing device. The communication interface 108 may be implemented as one or both of a wired network interface and a wireless network interface. The memory 110 is one or more of volatile memory (e.g., RAM) and non-volatile memory (e.g., ROM, FLASH, magnetic media, optical media, et cetera). In some examples, the memory 110 is also a non-transitory computer-readable medium. Although shown within the local identity server 104, memory 110 may be, at least in part, implemented as network storage that is external to the local identity server 104 and accessed via the communication interface 108. For example, all or part of memory 110 may be housed on the "cloud."

The optional global identity server 118 includes an electronic processor 120, a communication interface 122, and a memory 124. The electronic processor 120 is communicatively coupled to the communication interface 122 and the memory 124. The electronic processor 120 is a microprocessor or another suitable processing device. The communication interface 122 may be implemented as one or both of a wired network interface and a wireless network interface. The memory 124 is one or more of volatile memory (e.g., RAM) and non-volatile memory (e.g., ROM, FLASH, magnetic media, optical media, et cetera). In some examples, the memory 124 is also a non-transitory computer-readable medium. The memory 124 may be, at least in part, implemented as network storage that is external to the optional global identity server 118 and accessed via the communication interface 122. For example, all or part of memory 124 may be housed on the "cloud." Additionally, some or all of the functions attributed to the local identity server 104 may also be performed by the optional global identity server 118.

The biometrically-enhanced identity engine 112 may be stored within a transitory or non-transitory portion of the memory 110. The biometrically-enhanced identity engine 112 includes machine readable instructions that are executed by the electronic processor 106 to perform the functionality of the local identity server 104 as described below with respect to FIGS. 2–21.

The memory 110 may include a database 114 for storing information about individuals. The database 114 may be an RDF database, i.e., employ the

Resource Description Framework. Alternatively, the database 114 may be another suitable database with features similar to the features of the Resource Description Framework, and various non-SQL databases, knowledge graphs, etc. The database 114 may include a plurality of records (also referred to herein as a "data pod"). Each record may be associated with and contain personal information about one individual. For example, in the illustrated embodiment, record 116 may be associated with the individual 140, and other N records may be respectively associated with one of N other individuals (not expressly shown in FIG. 1).

The local partner device 130 may be web-compatible mobile computer, such as a laptop, a tablet, a smart phone, or other suitable computing device. Alternately, or in addition, the local partner device 130 may be a desktop computer. The local partner device 130 includes an electronic processor in communication with memory. In an embodiment, the electronic processor of the computer 130 is also in communication with a biometric scanner via a communication interface. In another embodiment, the biometric scanner may be part of the local partner device 130. The electronic processor is a microprocessor or another suitable processing device, the memory is one or more of volatile memory and non-volatile memory, and the biometric scanner is one or more biometric scanning devices (e.g., a device that scans fingerprints, facial features, irises, handwriting, etc.) now known or subsequently developed. The communication interface may be a wireless or wired network interface.

An application, which contains software instructions implemented by the electronic processor of local partner device 130 to perform the functions of the local partner device 130 as described herein, is stored within a transitory or a non-transitory portion of the memory. The application may have a graphical user interface that facilitates interaction between the individual 140 and the local identity server 104.

The local partner device 130 may include or be in communication with a point of sale system (POS), e.g., a mobile POS system (such as a mobile card reader). As discussed herein, the local partner device 130 may use the mobile POS system to, among other things, read a partner-specific identification asset (not shown and considered to be part of the block "individual 140") associated with the individual 140 to verify the identity of the individual 140.

The local partner device 130 may communicate with the local identity server 104 over the network 160. The network 160 is preferably (but not necessarily) a wireless network, such as a wireless personal area network, local area network, or other suitable network. The local partner device 130 may directly communicate with the local identity server 104 or indirectly communicate over network 160.

In an embodiment, the memory of the local partner device 130 may include a database and software. The database of the local partner device 130 may include information about individual 140 and other individuals, as set forth herein. The software of the local partner device 130 may facilitate interaction between the local partner device 130 and individuals (e.g., the individual 140) and allow for the local partner device 130 to track the interactions as described in greater detail below.

The local identity server 104 may likewise communicate with partner devices other than the local partner device 130. The term "partner", as used herein, encompasses any other organizations engaging with individuals, including but not limited to non-governmental organizations and other charitable institutions (including governmental organizations). The term "individual", as used herein, encompasses a person (or household) that seeks to interact with an organization or entity, including but not limited to seeking access to services (e.g., an individual in a refugee camp, a person who receives support, etc.). The workings of the local identity server 104 and the local partner device 130 will now be described in additional detail with FIGS. 2–21.

FIG. 2 is a block diagram illustrating a more detailed example 200 of the system 100 for securely identifying an individual, in accordance with various aspects of the present disclosure. In the example of FIG. 2, the example 200 includes an identity (ID) network/switch 202 that connects a local partner device 130 to the local identity server 104. The local partner device 130 is also connected to the optional global identity server 118.

The local partner device 130 includes an electronic processor and a memory. The memory includes a token translator 204, a unique user global unique identifier (GUID) generator 206, a distributed ledger 208, a biometric token creator 210, a local deduplication service 212, a token generator 214, biometric token libraries 216, and a local b-token storage 218.

The local identity server 104 includes an identity management service 220, a pod management service 222, a plurality of personal data stores 224 (also referred to as “data pods”), and a database file system 226.

The optional global identity server 118 includes an electronic processor and a memory. The memory includes a global deduplication service 228 and a global biometric token storage 230.

In the example of FIG. 2, the individual 140 consents to biometric capture by the local partner device 130. The local partner device 130 create a biometric token from the biometric capture of the individual 140 with the biometric token creator 210. The biometric token creator 210 creates a biometric token with a tokenization algorithm.

FIG. 3 is a flow diagram illustrating an example operation 300 of the system 100 of FIG. 1 for registering/enrolling the individual 140 in an identity network services platform, in accordance to various aspects of the present disclosure. In the example of FIG. 3, after capturing the biometrics of the individual 140 (at link 1), the local partner device 130 creates a unique and private global universal identifier (GUID) token with the unique GUID generator 206 (at link 2). In some examples, the unique and private GUID token is biometrically-derived from the captured biometrics. In other examples, the unique and private GUID token is not biometrically-derived. For example, the unique and private GUID token may simply be a random number.

Additionally, the local partner device 130 generates a biometric token from the captured biometrics and stores the biometric token in the local b-token storage 216 (at link 3A). The local partner device 130, in parallel to creating and storing the biometric token, also retrieves an assigned unique identifier that is associated with the owner of the local partner device 130 (at link 3B). The local partner device 130 receives the unique and private GUID token and creates, with the token generator 214, a relationship identifier token from the unique identifier associated with the owner and the unique and private GUID token (at links 3A and 3B).

In some examples, the local partner device 130 generates a high-level identifier “W” token from the relationship identifier token (at link 4). The high-level identifier “W” token is a pod identifier (e.g., WebID, DID, or another unique identifier) assigned to a new data pod. In other examples, the local partner device 130 may use the relationship identifier or the biometric token instead of the high-level identifier.

The local partner device 130 assigns a first pod identifier token, e.g., a webID, DID, or another unique identifier (at link 6). After assigning the pod identifier, the local partner device 130 creates a personal data store (also referred to as a "pod" or "data pod") by creating a second pod identifier token (i.e., a p-ID) that is tied to a pivot table (at link 7). The pivot table stores various information in the pod, e.g., the biometric token, the first pod identifier token, the second pod identifier token, and/or other suitable information.

In parallel to links 3A–7, the local partner device 130 receives the biometric token, the GUID token, and information regarding the type of biometric capture from the local partner device 130 (at link 8). In response to receiving the biometric token, the GUID token, and the information regarding the type of biometric capture, the local partner device 130 creates a personalized packet and a QR code. After creating the personalized packet, the local partner device 130 issues a smartcard or other identification vehicle that includes the high-level identifier, the biometric token, the unique and private GUID token (at links 9 and 10).

Lastly, FIG. 3 is described with respect to the local partner device 130. However, FIG. 3 is limited to being performed by the local partner device 130. Instead, FIG. 3 may also performed at least in part by the local identity server 104. For example, after receiving the biometrics of the individual 140 that are captured, the local identity server 104 may perform all of the functions described above with respect to the local partner device 130.

In a different example, the local identity server 104 may receive the high-level identifier, the biometric token, the unique and private GUID token, and the local identity server 104 creates a personalized packet and a QR code. After creating the personalized packet, the local identity server 104 issues a smartcard or other identification vehicle that includes the high-level identifier, the biometric token, the unique and private GUID token (at links 9 and 10).

FIG. 4 is a diagram illustrating a comparison between conventional verification of presence and inclusive verification of presence 400, in accordance with various aspects of the present disclosure. Conventionally, as illustrated in FIG. 4, a user takes a user identification (ID) card to a merchant, service provider, government, or non-governmental organization. A digital credential and/or data is recorded on a user's smart device and in the cloud against the specific user ID card. Lastly, specific identification documents must be present at the time of verification. Thus, the conventional verification of presence requires an online connection, an identification document, a digital credential, and the user's smart device.

With respect to the inclusive verification of presence 400, the user 140 may go to a merchant, service provider, government, or non-governmental organization without a user ID card and without a user's smart device. The merchant, service provider, government, or non-governmental organization uses a biometric capture device to capture biometrics of the user 140. A secure biometric token is created by the biometric capture device or other smart device with a biometric token generation application that receives biometrics from the biometric capture device.

In the inclusive verification of presence 400, the biometric capture device or other smart device may generate a QR code with an embedded form of the secure biometric token that is created. The QR code may also include other status data available for offline use.

Additionally, the biometric capture device or other smart device may send the secure biometric token to a user-managed, portable, and interoperable data pod, electronic wallet, or virtual account. In other words, the biometric capture device or other smart device makes the secure biometric token available both locally and globally.

The inclusive verification of presence 400 has several advantages over the conventional verification of presence. First, the inclusive verification of presence 400 is available both online and offline. Second, the inclusive verification of presence 400 does not require any identification documents. Third, the inclusive verification of presence 400 does not require any blockchain or distributed ledger. Fourth, the inclusive verification of presence 400 is not affected by lost or stolen identification documents. Fifth, the biometric capture device at the merchant, service provider, government, or non-governmental organization may be any biometric acceptance device (e.g., smartphones, tablets, or other suitable biometric acceptance devices).

The advantages of the inclusive verification of presence 400 is from biometric tokenization. By capturing biometrics and embedding biometric tokens (associated with the buyer, i.e., the individual 140) in a QR code, which may be put on the card itself and linked with the prepaid card details (on QR code, and on the issuer's backend). The biometric tokens may also issued via some other digital means and linked to the specific, issued prepaid card.

The individual 140 may verify ownership of the prepaid card against the QR code on the card. Additionally, the QR code lists last four digits of the prepaid card to show it is "linked" to that card, although any means to link the QR code to the prepaid card may be used.

The individual 140 may also regain the prepaid card balance the prepaid card is lost or stolen because the individual 140 may demonstrate ownership of that prepaid card. Moreover, the prepaid card issuer is able to store or access the link between biometric token and prepaid card.

FIG. 5 is a diagram illustrating a comparison between conventional verification of presence with a financial product and inclusive verification of presence 500 with a financial product, in accordance with various aspects of the present disclosure. Conventionally, as illustrated in FIG. 5, a user takes a payment card or payment device to a merchant, service provider, government, or non-governmental organization. A payment is made with the payment card or the payment device and a single use prepaid card is issued to the individual. Thus, the conventional verification of presence requires an online connection, an identification document, a digital credential, and the user's smart device.

With respect to the inclusive verification of presence 500, the user 140 may go to a merchant, service provider, government, or non-governmental organization without a payment card or a payment device. The merchant, service provider, government, or non-governmental organization uses a biometric capture device to capture biometrics of the user 140. A secure biometric token is created by the biometric capture device or other smart device with a biometric token generation application that receives biometrics from the biometric capture device.

In the inclusive verification of presence 500, the biometric capture device or other smart device may generate a QR code with an embedded form of the secure biometric token that is created. The QR code may also include virtual payment account information that is available for both online and offline use.

Additionally, the biometric capture device or other smart device may be embedded into a reusable prepaid card issued to the individual 140. In other words, the biometric capture device or other smart device makes a virtual account or a reusable prepaid card available and verifiable online and offline.

The inclusive verification of presence 500 has several advantages over the conventional verification of presence. First, the inclusive verification of presence 500 is available both online and offline. Second, the inclusive verification of presence 500 does not require any identification documents. Third, the inclusive verification of presence 500 does not require any blockchain or distributed ledger. Fourth, the inclusive verification of presence 500 is not affected by lost or stolen reusable prepaid cards. Fifth, the biometric capture device at the merchant, service provider, government, or non-governmental organization may be any biometric acceptance device (e.g., smartphones, tablets, or other suitable biometric acceptance devices). Sixth, the prepaid card is reloadable and reusable and meets some know-your-customer (KYC) requirements.

FIG. 6 is a flow diagram illustrating an example 600 for issuing a digital identity credential of a registered individual with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure. In example 600 of FIG. 6, the individual 140 registers a computing device 602 (e.g., a computing device as illustrated in FIG. 6) with a service provider. The service provider is an owner of the local partner device 130 as described above in FIG. 1.

The individual 140 receives a PIN and completes registration of the computing device 602 with a USSD Gateway operator 604 based on session information. The completed registration with the USSD Gateway operator 604 authorizes the computing device 602 to receive biometric registration. In some examples, operators other than the USSD Gateway operator 604 may be used.

The individual 140 then presents the registered computing device 602 to the service provider. The service provider captures biometrics of the individual 140 with the local partner device 130 as described above in FIG. 1.

In response to capturing the biometrics of the individual 140, the local partner device 130 creates a unique data account (e.g., a data pod as described above in FIG. 3). Additionally, in response to capturing the biometrics of the individual, the local partner device 130 generates a biometric token, associates the biometric token with the unique data account, and issues the biometric token as a USSD code via a USSD session. For example, the USSD code may be *122#.

In some examples, the example 600 may be a farmer enrolling in an e-voucher program that requires use of a phone for access to services. The farmer receives a unique code based on the farmer's biometrics on the phone for future verifications.

Additionally, in some examples, the biometric token may be too large to store on a feature phone via a USSD menu. In these examples, a web link or a pointer to the place where the biometric token is stored may be used instead of the biometric token via the USSD menu. The web link or a pointer may be facilitated with a mobile wallet and the USSD menu. Specifically, the individual 140 may have his/her biometric tokens captured and stored in a location that is shared with the individual 140 via the USSD menu and the mobile wallet access, and perhaps link to other data about the individual 140. In these examples, once the individual 140 successfully verifies against the stored biometric token "living" behind a web link/pointer, only then will other personal data associated with the individual 140 will be shared or released.

FIG. 7 is flow diagram illustrating example 700 for registering and accessing decentralized points of service with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 700 of FIG. 7, the individual 140 registers with a service provider by providing biometrics to the service provider. The service provider captures the biometrics of the individual 140 with the local partner device 130 as described above in FIG. 1. The local partner device 130 generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 executes a data orchestration service 702 to distribute the biometric token to the cloud and one or more local devices via a local data exchange network 704. The one or more local devices are additional decentralized points of service.

In the example 700 of FIG. 7, a second local partner device 706 (similar to the local partner device 130 of FIG. 1) associated with a second service provider receives the biometric token either locally from the local partner device 130 or from the cloud via the local data exchange network 704. The second local partner device 706 updates the b-token storage to include the biometric token from the local partner device 130.

In the example 700 of FIG. 7, the individual 140 accesses services from the second service provider by providing biometrics to the second service provider. The second service provider captures the biometrics of the individual 140 with the second local partner device 706. The second local partner device 706 generates a second biometric token based on the captured biometrics. In some examples, the biometrics provided to the second service provider is a QR code generated by the local partner device 130 and indicative of the distributed biometric token.

In response to generating the second biometric token, the second local partner device 706 compares the second biometric token to tokens stored in the local b-token storage. The second local partner device 706 confirms an identity of the policy member when the second biometric token substantially matches the biometric token that was distributed and stored in the local b-token storage.

In the example of FIG. 7, rather than storing biometric tokens centrally, in the cloud, the local partner device 130 or the local identity server 104 may distribute biometric tokens to mobile devices or keep the biometric tokens created on that mobile device, instead of just sending that data to the cloud. In other words, the local partner device 130 or the local identity server 104 may create a distributed version of the central cloud-based biometric token vault.

Additionally, in some cases, the distribution of personal data is unnecessary and only a biometric token is necessary. For example, the biometric token may represent "membership" in a particular program or association with a particular entity, so that any person matching that biometric token is the individual 140 and allowed to receive certain benefits based on the relationship between the individual and the particular program or the particular entity.

Further, in some examples, the registration process of FIG. 7 includes pre-registration for individuals that do not have all documents at the time of registration with a particular entity (for example, banks in rural areas via traveling registration vehicles). The particular entity may, with the local partner device 130 (e.g., a mobile device or a registration terminal), register the person, collect other relevant data, and bind the entire application to one or more biometric token(s) when identity (ID) documents are insufficient. When the pre-registration is in complete, the individuals may continue the application in the future when the same person (matching the biometric tokens) shows up at the particular entity to continue the registration process.

Furthermore, in some examples, the registration process of FIG. 7 may involve a plurality of local partner devices including the local partner device 130. In these examples, the plurality of local partner devices may sync biometric tokens with each other when online or communicatively connected to each other. The syncing of biometric tokens with each other reduces or eliminates a possibility of registering the individual 140 more than once even when the local partner device 130 is offline. In some examples, the plurality of local partner device may sync by proximity using Bluetooth®, a physical cable, Wi-Fi, or other suitable communication means.

FIG. 8 is flow diagram illustrating example 800 for registering and accessing healthcare with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 800 of FIG. 8, the individual 140 purchases health insurance from a health insurance provider by providing biometrics to an agent of the health insurance provider. The agent captures the biometrics of the individual 140 with the local partner device 130 as described above in FIG. 1. The local partner device 130 generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 executes a data orchestration service 802 to distribute the biometric token to the cloud and one or more local devices via a local data exchange network 804. The one or more local devices are computing devices located at various healthcare facilities that are associated with the health insurance provider.

In the example 800 of FIG. 8, a second local partner device 806 (similar to the local partner device 130 of FIG. 1) associated with one of the healthcare facilities receives the biometric token either locally from the local partner device 130 or from the cloud via the local data exchange network 804. The second local partner device 806 updates the b-token storage to include the biometric token from the local partner device 130.

In the example 800 of FIG. 8, the individual 140 accesses services from the one of the healthcare facilities by providing biometrics to the healthcare facility. The healthcare facility captures the biometrics of the individual 140 with the second local partner device 806. The second local partner device 806 generates a second biometric token based on the captured biometrics. In some examples, the biometrics provided to the healthcare facility is a QR code generated by the local partner device 130 and indicative of the distributed biometric token.

In response to generating the second biometric token, the second local partner device 806 compares the second biometric token to tokens stored in the local b-token storage. The second local partner device 806 confirms an identity of the policy member when the second biometric token substantially matches the biometric token that was distributed and stored in the local b-token storage.

FIG. 9 is flow diagram illustrating example 900 for registering for healthcare with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 900 of FIG. 9, the individual 140 registers for health service by providing biometrics to an agent of a health service provider. The health service provider captures the biometrics of the individual 140 with the local partner device 130 as described above in FIG. 1. The local partner device 130 generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 executes a data orchestration service 902 to distribute the biometric token to the cloud and one or more local devices via a local data exchange network 904. The one or more local devices are computing devices located at various healthcare facilities that are associated with the health service provider.

In the example 900 of FIG. 9, a second local partner device 906 (similar to the local partner device 130 of FIG. 1) associated with one of the healthcare facility receives the biometric token either locally from the local partner device 130 or from the cloud via the local data exchange network 904. The second local partner device 906 updates the b-token storage to include the biometric token from the local partner device 130.

In the example 900 of FIG. 9, the individual 140 accesses services from the healthcare facility by providing biometrics to the healthcare facility. The healthcare facility captures the biometrics of the individual 140 with the second local partner device 906. The second local partner device 906 generates a second biometric token based on the captured biometrics. In some examples, the biometrics provided to the healthcare facility is a QR code generated by the local partner device 130 and indicative of the distributed biometric token.

In response to generating the second biometric token, the second local partner device 906 compares the second biometric token to tokens stored in the local b-token storage. The second local partner device 906 confirms an identity of the policy member when the second biometric token substantially matches the biometric token that was distributed and stored in the local b-token storage.

FIG. 10 is flow diagram illustrating examples 1000 and 1050 for biometrically-enhancing data exchange and records matching with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1000 of FIG. 10, the individual 140 registers with a health service provider by providing biometrics to the health service provider. For example, the individual 140 adds an authorized user with limited delegation of authority.

The health service provider captures the biometrics of the individual 140 with the local partner device 130 as described above in FIG. 1. The local partner device 130 generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 creates or updates a data account 1002 that is unique to the individual. The local partner device 130 also updates a data pod 1004 associated with the individual 140 to include the biometric token and the authorized user information.

In the example 1050 of FIG. 10, with consent of the individual 140, a first health provider sends records to a second health provider. The records have some personally-identifiable information (PII) removed, e.g., date-of-birth, address, and name. However, the records each include a biometric token associated with the individual 140.

In response to receiving the records, the second health provider uses a second local partner device 1006 to match 1052 the biometric tokens in the records to one or more data pods or other records of the individual 140. The second local partner device 1006 then confirms a match 1054 when the match probability is a high probability (the high probability defined by industry standard or by service provider). Once a match has been confirmed, the second local partner device 1006 performs de-duplication 1056 of data between the matching records.

Matching of patient records using biometrics is a long-time ‘dream’ in healthcare industry but marred with challenges including some privacy risks. Moreover, biometric templates and biometric images are large, and considered very sensitive.

Conventionally, merging or sharing of medical records between two medical providers fails 50% of the time because of data errors, misspellings, missing data elements. Moreover, many medical providers do not use biometrics to match records because it presents some risks and both medical providers must use the same biometric vendor.

The examples 1000 and 1050 provides a number of distinct advantages. First, the size of the biometric tokens allows for embedding multiple biometric tokens into printed and digital medical records (for flexibility, as an as higher level of assurance). Second, the biometric tokens provide layered privacy because biometrics tokens of a face may be used for less sensitive records and biometric tokens of a palm may be embedded into more sensitive records, where you need my physical presence versus capturing my face on the street or using a facial photo. Third, even if data is wrong, missing, or misspelled, the biometric tokens in the records between different hospitals may still be matched with a "presence." Fourth, medical providers may provide medical help to individuals that intentionally or unintentionally give incorrect data and match them against other records for a more complete medical history. Fifth, medical provides may provide medical help to known individuals that are unconscious or unwilling to communicate and match them against other records for a more complete medical history. Sixth, appending biometric tokens to medical files/records is lower risk than biometric images/templates because biometric tokens may be revoked and are more secure than the biometric images/templates. Seventh, biometric matching may be used to fix data inaccuracy and/or misspellings for records with a very strong biometric match. Lastly, and most importantly, the choice of biometric vendor may be given to the individual 140 because the individual 140 may work with one partner to capture biometrics, generate tokens, and give the biometric tokens to each respective hospital for the purpose of appending to the medical record. Then, the individual 140 is at the center of the data exchange rather than the medical provider.

FIG. 11 is flow diagram illustrating examples 1100 and 1150 for paying for items using biometrics versus smartphone with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1100 of FIG. 11, the individual 140 scans in items and completes checkout by providing biometrics to the local partner device 130 (e.g., a checkout terminal). The local partner device 130 captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics. In response to generating the biometric token, the local partner device 130 sends the biometric token to the local identity server 104 (e.g., a server administered by a bank) via an identity and payments network 1102.

The local identity server 104 matches the biometric token that is received from the local partner device 130 to a data pod 1104. The local identity server 104 confirms whether authorization to make a payment at the local partner device 130 exists in the data pod 1104. When the authorization exists, the local identity server 104 generates a payment token that approves the transaction at the local partner device 130 and sends the payment token to the local partner device 130 via the identity and payments network 1102.

In example 1150 of FIG. 11, the individual 140 scans in items and completes checkout by activating an identity verification service on the local partner device 130 (e.g., an identity verification service application on the individual's smartphone). The local partner device 130 includes a digital wallet and biometric modalities and requests a biometric capture of the individual 140.

The local partner device 130 captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics. The local partner device 130 verifies the biometric token that is generated matches a pre-existing token stored in the memory of the local partner device 130. In response to verifying the biometric token, the local partner device 130 sends the biometric token to the local identity server 104 (e.g., a server administered by a bank) via an identity and payments network 1102.

The local identity server 104 matches the biometric token that is received from the local partner device 130 to a data pod 1104. The local identity server 104 confirms whether authorization to make a payment at the local partner device 130 exists in the data pod 1104. When the authorization exists, the local identity server 104 generates a payment token that approves the transaction at the local partner device 130 and sends the payment token to the local partner device 130 via the identity and payments network 1102.

In summary of FIG. 11, biometric tokens may be created and embedded into a digital account (referred to herein as a "data pod") that belongs to the individual 140. The data pod includes payment tokens, identity data, and/or other data associated with the individual 140. Successful authentication into the data pod using one or more biometric token(s) may be used to unveil the link to payment information, to process the transaction.

FIG. 12 is flow diagram illustrating examples 1200 and 1250 for payment with secure biometrics and one-time credentials with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1200 of FIG. 12, the local partner device 130 captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics. In response to generating the biometric token, the local partner device 130 sends the biometric token to the local identity server 104 (e.g., a server administered by a bank) via an identity and payments network 1202.

The local identity server 104 matches the biometric token that is received from the local partner device 130 to a data pod 1204. The local identity server 104 confirms whether authorization to make a payment at the local partner device 130 exists in the data pod 1204 or whether the data pod 1204 includes an identification of payment pod 1206 associated with the individual 140. When the authorization exists in the data pod 1204, the local identity server 104 generates a payment token that approves the transaction at the local partner device 130 and sends the payment token to the local partner device 130 via the identity and payments network 1102.

When the identification of payment pod 1206 associated with the individual 140 exists in the data pod 1204, the local identity server 104 requests payment authorization from the payment pod 1206 via the identity and payments network 1202. In the example of FIG. 12, the payment pod 1206 is located at another server external to the local identity server 104. For example, the payment pod 1206 may be located in a server 1208 of another bank. However, in other examples, the payment pod 1206 may also be located on the local identity server 104 and/or the optional global identity server 118. When the authorization exists in the payment pod 1206, and in response to receiving the payment authorization, the server 1208 generates a payment token that approves the transaction at the local partner device 130 and sends the payment token to the local partner device 130 via the identity and payments network 1202.

In example 1250 of FIG. 12, the individual 140 completes checkout by activating an identity verification service on the local partner device 130 (e.g., an identity verification service application on the individual's smartphone). The local partner device 130 includes a digital wallet, biometric modalities, and a payment credential. The local partner device 130 requests a biometric capture of the individual 140.

The local partner device 130 captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics. The local partner device 130 verifies the biometric token that is generated matches a pre-existing token stored in the memory of the local partner device 130. In response to verifying the biometric token, the local partner device 130 sends the biometric token and the payment credential to the local identity server 104 (e.g., a server administered by a bank) via an identity and payments network 1202.

The local identity server 104 matches the biometric token that is received from the local partner device 130 to the data pod 1204. The local identity server 104 confirms whether authorization to make a payment at the local partner device 130 exists in the data pod 1204 or whether the data pod 1204 includes an identification of the payment pod 1206 associated with the individual 140. When the authorization exists in the data pod 1204, the local identity server 104 generates a payment token that approves the transaction at the local partner device 130 and sends the payment token to the local partner device 130 via the identity and payments network 1202.

When the identification of payment pod 1206 associated with the individual 140 exists in the data pod 1204, the local identity server 104 requests payment authorization from the payment pod 1206 via the identity and payments network 1202. In the example of FIG. 12, the payment pod 1206 is located at another server external to the local identity server 104. For example, the payment pod 1206 may be located in the server 1208 of another bank. However, in other examples, the payment pod 1206 may also be located on the local identity server 104 and/or the optional global identity server 118. When the authorization exists in the payment pod 1206, and in response to receiving the payment authorization, the server 1208 generates a payment token that approves the transaction at the local partner device 130 and sends the payment token to the local partner device 130 via the identity and payments network 1202.

In summary of FIG. 12, successful biometric authentication leads to a one-time credential or token. Further, the digital data pod may have varying rules. For example, when a facial biometric token is used to authenticate, then only transactions up to $250 may be authorized. However, when a palm biometric token is used to authenticate, then transactions over $250 may be authorized.

FIG. 13 is flow diagram illustrating examples 1300 and 1350 for smart checkout with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1300 of FIG. 13, the individual 140 provides a credit card to a computing device 1302 to enroll in click for pay with the credit card. The individual 140 also provides biometrics to the local partner device 130 (e.g., the computing device 1302 or some other suitable computing device that captures biometrics), which captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 sends the biometric token and the payment details as enrollment data to the local identity server 104 (e.g., a server administered by a bank) via an identity and a payments network. In response to receiving the enrollment data, the local identity server 104 creates a payments pod 1304 including the biometric token and payments token.

In example 1350 of FIG. 13, the individual 140 activates an identity service on the local partner device (e.g., a smartphone) to enroll in click for pay. The individual 140 also provides biometrics to the local partner device 130, which captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 sends the biometric token and the payment details as enrollment data to the local identity server 104 (e.g., a server administered by a bank) via an identity and payments network 1352. In response to receiving the enrollment data, the local identity server 104 creates a payments pod 1304 including the biometric token and a payments token.

In the example of FIG. 13, the biometric token may be linked to, or inside of, a secure remote commerce (SRC) account. Further, multiple rules may be set in place with respect to the SRC account. For example, when the individual 140 is present, and biometrically authenticated, only then will an online transaction for $10,000+ will go through (limits set by the individual 140).

One primary advantage of the biometric token is an additional level of assurance for some transactions and/or interactions. For example, the biometric token enables card-less payments online, that is, the individual 140 does not need to enter card details. Instead, the individual 140 may simply authenticate biometrically to your SRC account.

Another advantage of the biometric token is an excellent defense against an "account takeover." Moreover, while biometric templates and biometric images may provide a similar defense against an "account takeover," biometric images and biometric templates are very sensitive data and pose a significant risk even when sent encrypted.

The biometric token may still be used to biometrically authenticate the individual 140. However, the biometric token is useless random data to any one that views the biometric token.

Further, there are very few rules in place on transaction size, links to specific and deliberate user agreement (for highest value transactions). Most high value transactions are expected to be carried out via ACH, wire transfer, check, but not often debit cards or credit cards. In other words, the biometric token may provide proof of presence and proof of liveness behind a given SRC transaction.

Yet another advantage is that the biometric tokens will allow the individual 140 to link together different SRC accounts. Conventionally, each SRC implementation is a standalone SRC account. The individual 140 must sign up for more than one SRC account if the individual 140 plans to shop via SRC with more than one payment processor. However, the biometric token may be used to allow the individual 140 to access SRC accounts across all payment processors.

FIG. 14 is flow diagram illustrating examples 1400 and 1450 for checking out using an application versus biometrics only with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1400 of FIG. 14, the individual 140 activates a store application on the local partner device 130 (e.g., a smartphone). The individual 140 also provides biometrics to the local partner device 130, which captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics.

In response to generating the biometric token, the local partner device 130 authenticates the biometric token to confirm the identity of the individual 140 and generates a dynamic QR code that confirms the use of the store application on the local partner device 130. In response to generating the dynamic QR code, the individual 140 presents the dynamic QR code to a scanner 1402.

In response to scanning the dynamic QR code, the scanner 1402 controls a presence detection device 1404 (e.g., a camera or camera system) to track the presence and shopping of the individual 140 based on the dynamic QR code that points to the shopping application of the local partner device 130. In some examples, the presence detection device 1404 tracks the presence and shopping of the individual 140 by generating a temporary biometric token by scanning the face or other distinguishing body part of the individual 140 and connecting any items retrieved by the individual 140 to the temporary biometric token.

Once the presence detection device 1404 detects the individual 140 leaving the store, the presence detection device 1404 communicates the retrieved items to the scanner 1402 and deletes the temporary biometric token. In response to receiving the retrieved items from the presence detection device 1404, the scanner 1402 charges the local partner device 130 for the retrieved items. In response to receiving a charge from the scanner 1402, the local partner device 130 charges a credit card on file in the store application of the local partner device 130.

In example 1450 of FIG. 14, the individual 140 has previously enrolled in payment authorization with a merchant using a first biometric token. The individual 140 provides biometrics to the local partner device 130 (e.g., a turnstile scanner), which captures the biometrics of the individual 140 and generates a dynamic biometric token based on the captured biometrics. The local partner device 130 confirms the dynamic biometric token authenticates the individual 140 by comparing the dynamic biometric token to the first biometric token.

In response to determining that the individual 140 is authenticated and has previously enrolled in payment authorization, the local partner device 130 controls the presence detection device 1404 (e.g., a camera or camera system) to track the presence and shopping of the individual 140. In some examples, the presence detection device 1404 tracks the presence and shopping of the individual 140 by generating a temporary biometric token by scanning the face or other distinguishing body part of the individual 140 and connecting any items retrieved by the individual 140 to the temporary biometric token.

Once the presence detection device 1404 detects the individual 140 leaving the store, the presence detection device 1404 communicates the retrieved items to the local partner device 130 and deletes the temporary biometric token. In response to receiving the retrieved items from the presence detection device 1404, the local partner device charges a credit card or digital wallet on file from enrollment by the individual 140.

In the example of FIG. 14, the partner does not need to store biometric images or biometric templates in a local or a central ecosystem, which leads to fewer cybersecurity and data privacy risks. Additionally, the example 1400 may use a more "private" biometric modality like a palm scan to initiate and authorize creation of a stronger credential with a higher level of assurance (e.g., for the purpose of entering the store and initiating the purchase experience).

In summary, the local partner device 130 links a palm biometric token (instead of a facial biometric token) to the payment details (stored as a payment token and/or credit card information). The local partner device 130 may bind the palm biometric token from the QR code with the facial biometric token collected at the time of the entrance to the shopping area (e.g., at the turnstile).

The local partner device 130 may use facial recognition technology and the presence detection device 1404 to track purchases and determine when the user is leaving the purchase area. Lastly, the local partner device 130 may retrieve the face to palm link to process a payment.

One advantage of the example 1400 is that the local partner device 130 may an application deployed on any smart device with a regular camera. Another advantage is that the application only uses biometric tokens versus encrypted biometric templates sent to the cloud. Yet another advantage of the example 1400 is a more secure local storage on the mobile device – as the risks associated with biometric tokens are extremely small compared to biometric templates or biometric images – and allows the example 1400 to be deployed in an offline environment when the individual 140 has pre-registered biometrically.

FIG. 15 is flow diagram illustrating an example 1500 of creating or updating user-centric data pods with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1500 of FIG. 15, the individual 140 visits a partner and provides biometrics to the local partner device 130, which captures the biometrics of the individual 140 and generates a biometric token based on the captured biometrics. In response to generating the biometric token, the local partner device 130 captures registration data from the individual 140. The registration data may include personal data, consent data rights, one or more privacy notices, communications, payment credentials, or other suitable registration data.

In response to capturing the registration data, the local partner device 130 uses a data orchestration service 1502 to create or update a digital data pod 1504. The digital data pod 1504 may be created and located on any one of the local partner device 130, the local identity server 104, the optional global identity server 118, or some combination thereof. When the digital data pod 1504 is created and located on the local partner device 130, the local partner device 130 may synchronize with the local identity server 104 and/or the optional global identity server 118 to also create and maintain the digital data pod 1504. In some examples, the local partner device 130 may be a smartphone in the possession of the individual 140.

When the digital data pod 1504 is located on the local partner device 130, the local partner device 130 may share data included in the digital data pod 1504 with one or more third-parties 1506 and 1508 when the individual 140 has provided consent to sharing data to third-parties. When the digital data pod 1504 is located on the local identity server 104, the local identity server 104 may share data included in the digital data pod 1504 with one or more third-parties 1506 and 1508 when the individual 140 has provided consent to sharing data to third-parties. When the digital data pod 1504 is located on the optional global identity server 118, the optional global identity server 118 may share data included in the digital data pod 1504 with one or more third-parties 1506 and 1508 when the individual 140 has provided consent to sharing data to third-parties.

Optionally, in some examples, the digital data pod 1504 may be connected to a physical identification or payment card via a biometric token stored in the digital data pod 1504. In these examples, when the digital data pod 1504 also includes payment credentials, then the digital data pod 1504 is also considered a "payment pod" as described herein.

FIG. 16 is flow diagram illustrating an example 1600 authorizing data sharing from the digital data pod 1504 of FIG. 15 using a consent management module, in accordance to various aspects of the present disclosure. In the example of FIG. 16, the individual 140 receives a request to share select data elements from a program owner 1602, a community pass third-party 1604, or a non-community pass third-party 1606 (at link 1). When the request comes from the non-community pass third-party 1606, the community pass network trust scheme review validation occurs in parallel to the request to reduce or eliminate spam or fraud (at links 2 and 3).

The individual 140 may deny data sharing to any of the requests (at link 4). The individual 140 may also approve of data sharing to any of the requests (at link 5).

When the individual 140 approves of data sharing (at link 5), the individual 140 must provide biometrics to generate a biometric token. The biometric token that is generated allows a computing device to identify to the digital data pod 1504 that is associated with the individual 140. Upon identifying the digital data pod 1504, the computing device retrieves authorization requirements for data sharing from the digital data pod 1504. When biometric verification is one of the authorization requirements, the computing device may perform biometric verification with the biometric token that was generated and a second biometric token stored with the digital data pod 1504 (at link 6).

Once the computing device has satisfied the authorization requirements, the computing device may either access the PII data from the digital data pod 1504 or retrieve a pointer that points to a PII data pod 1608 that stores PII data of the individual 140. In the example of FIG. 16, after retrieving the pointer, the computing device may access the PII data pod 1608 (at link 7).

Once the computing device has accessed the PII data pod 1608, the computing device may access different types of PII (at link 8). For example, the computing device may access PII data element groups including finance, demographics, and health. The computing device may also access more sensitive PII data including a health status, social security number, vulnerability, or other highly sensitive PII data.

After accessing the PII data in the PII data pod 1608, the computing device may share any PII data elements with the community pass program owner 1602 (at link 9). The computing device may share only some of the PII data elements with the community pass third-party 1604 (at link 9). Lastly, the computing device may share only select PII data elements with a non-community pass third-party 1606 with the consent of the individual 140 (at link 9).

A digital existence of the individual 140 needs the ability to share data (verified & unverified) with respective service providers. This data may reside at different service providers (i.e., health, utility, bank, etc.). The example 1600 provides the individual 140 control and only the individual 140 may authorize such exchange of data (unless another person has been authorized by the individual 140), and reduces or eliminates any violation of the privacy of the individual 140. The example 1600 addresses the disadvantages of conventional sharing of data because the conventional sharing of this data with new service providers is visible to all parties involved and also prone to man-in-the-middle attacks or other similar attacks.

FIG. 17 is flow diagram illustrating an example 1700 authorizing time-limited data sharing from the digital data pod 1504 of FIG. 15 using a consent management module, in accordance to various aspects of the present disclosure.

In the example of FIG. 17, one of third-parties 1602–1606 presents a JSON-web token the local identity server 104 authorizing access to select data elements of the digital data pod 1504 (at link 1). The local identity server 104 validates the JSON-web token (at link 2). In response a validating the JSON-web token, the local identity server 104 initiates a data request to a digital data pod 1708 (at link 3). In response to initiating the data request, the local identity server 104 matches and finds a community pass account (i.e., the digital data pod 1708) (at link 4). After finding the community pass account, the local identity server 104 initiates the identity management service to process pod access (at link 5).

Additionally, the local identity server 104 executes a pod management service to retrieve access requirements (at link 6). In the example of FIG. 17, the local identity server 104 determines that the digital data pod 1708 is a biometric data pod with biometric token data only (at link 7). After determining that the data pod 1708 is a biometric data pod with the biometric token data only, the local identity server 104 re-validates the JSON-web token (at link 8).

After re-validating the JSON-web token, the local identity server 104 accesses the authorized data in the digital data pod 1504 with a relationship identifier that was included the digital data pod 1708 (at link 9). After accessing the authorized data, the local identity server 104 reads and retrieves the authorized data from the digital data pod 1504 (at link 10). Additionally, the local identity server 104 marks the authorized data in the digital data pod 1504 as shareable with the specific third-party requesting the authorized data (at link 11). After marking the authorized data as shareable to the specific third-party in the digital data pod 1504, the local identity server 104 executes a digital orchestration service 1710 to create and send an authorization token to one or more of the third-parties 1702–1706 (at link 12).

One or more of the third-parties 1702–1706 re-send the JSON-web token back to the local identity server 104 for re-validation along with the authorization token that includes the relationship identifier that identifies the digital data pod 1504 (at link 14). The local identity server 104 enables access to the one or more of the third-parties 1702–1706 in the digital data pod 1504 (link 15). After enabling access, the one or more third-parties gain access to the select pod data that is marked as shareable with the one or more third-parties 1702–1706 (at link 16).

Additionally, in parallel or subsequent to the one or more third-parties 1702–1706 obtaining access to the select pod data, a transaction history and content management data is updated in a ledger stored in the digital data pod 1504 by the local identity server 104 and the one or more third-parties 1702–1706 that accessed the digital data pod 1504 (at links 17 and 18). Lastly, access to the select pod data shared with the one or more third-parties 1702–1706 is either ended as a one-time link or continued as a live link to the digital data pod 1504 (at link 19).

In summary, with respect to the example 1700, only the individual 140 may authorize the use of their data and only the recipient or requester may see the data that is requested and authorized. The provider of the data cannot track the activity of the individual 140 and the network is blind the contents of the data that is requested and authorized.

FIG. 18 is flow diagram illustrating an example 1800 authorizing time-limited data sharing from the digital data pod 1504 of FIG. 15 using a consent management module, in accordance to various aspects of the present disclosure. FIG. 18 is similar to FIG. 17. Consequently, any redundant description is not repeated herein.

The difference between FIGS. 17 and 18 is a difference between allowing third-parties to access the digital data pod 1504 directly with one-time access or continuous access versus allowing third-parties to access a new, one-time digital data pod 1802 that may have a set expiration. For example, the one-time digital data pod 1802 may expire after a single access, after a set period of time, or other suitable expiration scheme. In other words, the difference between FIGS. 17 and 18 is the creation of a temporary digital data pod 1802.

In summary, with respect to the example 1800, on a successful authorization, a new temporary pod is created on the network. A new one-time encryption key is generated and authorized data is encrypted and stored in the temporary pod. The authorization token along with the encryption key and temporary pod location is sent to the data provider. The data provider writes the data to the temporary pod and encrypts the data. The authorization token, pod location and keys are sent to the requestor. The requestor retrieves the data and decrypts the data.

Additionally, access to sensitive personal data may be enabled via creation of one-time use data pods, which are linked to the main data pod for the individual 140. The data to be shared with a specific entity (approved by the individual 140) is then placed in a temporary data pod and the link is shared with the specific entity to access the data for a limited period of time. After that the data is no longer accessible, and the data pod and its link are destroyed. The link should not be reusable in the future. Alternatively, the access to the data pod could be permanently disabled.

FIG. 19 is flow diagram illustrating an example 1900 of an individual registering with a partner and establishing a data pod with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In example 1900 of FIG. 19, the individual 140 visits a partner and provides biometrics along with consent to the local partner device 130 (at links 1 and 2). Upon capturing the biometrics of the individual 140, the local partner device 130 generates a biometric token based on the captured biometrics. In response to generating the biometric token, the local partner device 130 confirms the uniqueness of the biometric token in the local biometric token (b-token) storage of the local partner device 130 (at link 3).

In response to confirming the uniqueness of the biometric token, the local partner device 130 stores the biometric token in the local b-token storage and captures registration data from the individual 140 (at links 3 and 4). The local partner device 130 requests the local identity server 104 to create a community pass account (at link 5).

After creating the community pass account, the local identity server 104 establishes authentication methods (at link 6). The local identity server 104 also executes the identity management service and the pod management service to create a data pod identifier (at links 7–9). The local identity server 104 then receives the data pod identifier (at link 10).

Additionally, in parallel to requesting the local identity server 104 to create the community pass account, the local partner device 130 stores the PII data locally (at link 11). After storing the PII data locally, the local partner device 130 also sends the PII data to the local identity server 104, and in particular, for receipt by the identity management service (at link 12).

In response to receiving both the data pod identifier and the PII data, the local identity server 104 creates a personal data store 1902 (also referred to as a personal data pod) (at link 13). The personal data store 1902 the PII data, the biometric token, and the pod identifier.

Additionally, in the example of FIG. 19, the local identity server 104 also creates to sub-pods: a first sub-pod that includes only the biometric token and points back to the personal data store 1902 and a second sub-pod with only the PII data (at link 14). After creating the sub-pods, the local identity server 104 provides the pod identifier and the community pass account identifier to the cloud 1904, and specifically, as an update shared with the community pass orchestration service 1906 (at link 15). Additionally, after creating the sub-pods, the local identity server 104 provides the pod identifier, the relationship identifier, and a service credential to the cloud 1904, and specifically, as key identifier data shared with the partner (i.e., the community pass program owner) (at link 15). Lastly, the local identity server 104 provides access of the personal data store 1902 to the individual 140 (at link 16).

In summary, with respect to the example 1900, every organization that the individual 140 interacts with may create data pods specific to the individual and under the complete control of the individual 140. After successful biometric authentication, the individual 140 may choose to vail of such personal storage of all or selective data of their interactions. This data pod may then be accessed by the individual 140 at a later time to access and/or share the data with other providers. All access to such data pods is biometrically authenticated and recorded prior to any access or sharing.

FIG. 20 is flow diagram illustrating an example 2000 of an individual registering with another partner and updating a data pod with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure. FIG. 20 is similar to FIG. 19. Consequently, any redundant description is not repeated herein.

The difference between FIGS. 19 and 20 is a difference between an account creation versus an account update. The individual 140 created a community pass account and the personal data store 1902 in FIG. 19. In the example of FIG. 20, the individual 140 provides a smart card to a second partner, where the smartcard identifies the personal data store 1902 with a pod identifier and includes a biometric token and a GUID. The local identity server 104 updates the community pass account and the personal data store 1902 to include new data, specifically, a new biometric token and new PII data (link 14). The local identity server 104 also updates the cloud 2004 by providing key identifier data to the first partner described in FIG. 19 (at link 17) and to the second partner described in FIG. 20 (at link 18). The key identifier data may include the pod identifier, a relationship identifier, and a service credential.

With respect to the example 2000, a previously enrolled user and PII data are shared with the new service provider. The example 2000 uses the biometrics tokens to track consent and authorization to pod data.

FIG. 21 is flow diagram illustrating an example 2100 of an individual accessing a data pod at a point of service with the system 100 of FIG. 1, in accordance to various aspects of the present disclosure.

In the example of FIG. 21, the individual 140 provides consent to a biometrics capture to a local partner device 130 (at links 1 and 3). The individual 140 may also provide a smartcard 2102 that is ready by the local partner device 130 of the partner (at link 2). The smartcard 2102 may include a first biometric token, a GUID, and a pod identifier. The local partner device 130 may verify that the individual 140 is the owner of the smartcard 2102 by generating a second biometric token from the captured biometrics and comparing it to the first biometric token (at link 1). The local partner device 130 may store the first and second biometric tokens, the GUID, and the pod identifier in local storage (at link 4).

The individual 140 may request access data stored in a data pod associated with the individual 140 (at link 5). The local partner device 130 may send a partner identifier and the pod identifier to the local identity server 104 to find a community pass account (at link 6). After finding the community pass account, the local identity server 104 may process pod access by executing an identity management service (at link 7). After executing the identity management service, the local identity server 104 retrieves access requirements from the pod management service (at link 8).

In the example of FIG. 21, a JSON-web token validation may be the access requirement for accessing the data pod. As illustrated in FIG. 21, the JSON-web token is retrieved from the biometric data pod that only includes biometric token data (at link 9). The local identity server 104 re-validates the JSON-web token (at link 10).

When the re-validation of the JSON-web token is not strong enough, then the local identity server 104 may request the local partner device 130 to re-verify the biometric presence of the individual 140 (at link 11). When the re-validation of the JSON-web token is strong enough, the local identity server 104 accesses the personal data store 2104 (at link 12). The local identity server 104 reads and retrieves the requested pod data from the personal data store 2104 (at link 13).

The local identity server 104 processes the pod data with the identity management service (at link 14). After processing the pod data with the identity management service, the local identity server 104 enables pod viewer capability via the community pass data orchestration service (at link 15). The individual 140 obtains access to the pod data at the point of service by viewing the pod data via the community pass data orchestration service (at link 16).

In summary, with respect to the example 2100, service providers may store transaction data and PII data in user-specific pods. The access to these user-specific pods are controlled and protected by biometric tokens from registration by the individual 140. The biometric tokens for matching will stored in the user–specific pod and allows the individual 140 to authenticate to the pod and manage their data.

FIG. 22 is flow diagram illustrating an example process 2200 for securely storing information of an individual, in accordance with various aspects of the present disclosure. FIG. 22 is described with respect to FIG. 1.

In the example of FIG. 22, the method 2200 includes receiving, with a local partner device 130, biometrics and registration information of an individual 140 (at block 2202). The method 2200 includes generating, with the local partner device 130 and a tokenization algorithm, a first biometric token based on the biometrics that are received (at block 2204). The method also includes creating, with the local partner device 130, a data account associated with the individual 140 in a memory, the data account including the registration information and the first biometric token (at block 2206). Lastly, the first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual 140 with the tokenization algorithm.

Many different arrangements of the various components depicted, as well as components not shown, are possible without departing from the spirit and scope of the present disclosure. Embodiments of the present disclosure have been described with the intent to be illustrative rather than restrictive. Alternative embodiments will become apparent to those skilled in the art that do not depart from its scope. A skilled artisan may develop alternative means of implementing the aforementioned improvements without departing from the scope of the present disclosure. It should thus be noted that the matter contained in the above description or shown in the accompanying drawings is to be interpreted as illustrative and not in a limiting sense.

CLAIMS

What is claimed is:

1. A system for securely storing information of an individual, the system comprising:

a local partner device including a first electronic processor, a first communication interface, and a first memory, the first electronic processor is configured to

receive biometrics and registration information of an individual,

generate, with a tokenization algorithm, a first biometric token based on the biometrics that are received, and

create a data account associated with the individual in the first memory, the data account including the registration information and the first biometric token,

wherein the first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual with the tokenization algorithm.

2. The system of claim 1, wherein the first electronic processor is further configured to create a second data account associated with the individual in the first memory, the second data account including only the copy of the first biometric token that links the second data account to the data account.

3. The system of claim 1, further comprising:

a local identity server including a second electronic processor, a second communication interface, and a second memory, the second electronic processor is configured to

receive the data account from the local partner device, and

create a distributed data account associated with the individual in the second memory, the distributed data account including the registration information and the first biometric token.

4. The system of claim 3, wherein the second electronic processor is further configured to create a second data account associated with the individual in the second memory, the second data account including only the copy of the first biometric token that links the second data account to at least one of the data account or the distributed data account.

5. The system of claim 1, further comprising:

a plurality of local partner devices, each including a second electronic processor, a second communication interface, and a second memory,

wherein the first electronic processor is further configured to control the first communication interface to synchronize the data account with the plurality of local partner devices, and

wherein each of the plurality of local partner devices is configured to create a distributed data account associated with the individual in a third memory, the distributed data account including the first biometric token and the registration information stored in the data account.

6. The system of claim 5, wherein the second electronic processor is further configured to create a second data account associated with the individual in the second memory, the second data account including only the copy of the first biometric token that links the second data account to at least one of the data account or the distributed data account.

7. The system of claim 1, wherein the data account expires after a set period of time, and wherein the first electronic processor is configured to

delete the data account after an expiration of the set period of time, or

permanently disable the data account after the expiration of the set period of time.

8. The system of claim 1, wherein the first electronic processor is further configured to

receive an input from the individual that revokes consent of the individual with respect to the data account

receive the second set of the biometrics of the individual;

generate the second biometric token from the second set of the biometrics of the individual that is received;

identify the individual and the data account by matching the second biometric token that is generated to the first biometric token that is stored in the data account, and

delete the data account or permanently disable the data account in response to receiving the input and identifying the data account.

9. A method for securely storing information of an individual, the method comprising:

receiving, with a local partner device, biometrics and registration information of an individual;

generating, with the local partner device and a tokenization algorithm, a first biometric token based on the biometrics that are received; and

creating, with the local partner device, a data account associated with the individual in a memory, the data account including the registration information and the first biometric token,

wherein the first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual with the tokenization algorithm.

10. The method of claim 9, further comprising:

creating, with the local partner device, a second data account associated with the individual in the memory, the second data account including only the copy of the first biometric token that links the second data account to the data account.

11. The method of claim 9, further comprising:

receiving, with a local identity server, the data account from the local partner device; and

creating, with the local identity server, a distributed data account associated with the individual in a second memory, the distributed data account including the registration information and the first biometric token.

12. The method of claim 11, further comprising:

creating, with the local identity server, a second data account associated with the individual in the second memory, the second data account including only the copy of the first biometric token that links the second data account to at least one of the data account or the distributed data account.

13. The method of claim 9, further comprising:

controlling, with the local partner device, a first communication interface to synchronize the data account with a plurality of local partner devices, and

wherein each of the plurality of local partner devices is configured to create a distributed data account associated with the individual in a third memory, the distributed data account including the first biometric token and the registration information stored in the data account.

14. The method of claim 13, wherein the each of the plurality of local partner devices is further configured to create a second data account associated with the individual in a second memory, the second data account including only the copy of the first biometric token that links the second data account to at least one of the data account or the distributed data account.

15. The method of claim 9, wherein the data account expires after a set period of time, the method further comprising:

deleting, with the local partner device, the data account after an expiration of the set period of time, or

permanently disabling, with the local partner device, the data account after the expiration of the set period of time.

16. The method of claim 9, further comprising:

receiving, with the local partner device, an input from the individual that revokes consent of the individual with respect to the data account;

receiving, with the local partner device, the second set of the biometrics of the individual;

generating, with the local partner device, the second biometric token from the second set of the biometrics of the individual that is received;

identifying, with the local partner device, the individual and the data account by matching the second biometric token that is generated to the first biometric token that is stored in the data account; and

deleting or permanently disabling, with the local partner device, the data account in response to receiving the input and identifying the data account.

17. A non-transitory computer-readable medium comprising instructions that, when executed by an electronic processor, cause the electronic processor to perform a set of operations comprising:

receiving, with a local partner device, biometrics and registration information of an individual;

generating, with the local partner device and a tokenization algorithm, a first biometric token based on the biometrics that are received; and

creating, with the local partner device, a data account associated with the individual in a memory, the data account including the registration information and the first biometric token,

wherein the first biometric token is different from a biometric image or a biometric template in that the first biometric token only matches a copy of the first biometric token or a second biometric token that is generated from a second set of the biometrics of the individual with the tokenization algorithm.

18. The non-transitory computer-readable medium of claim 17, wherein the set of operations further includes

controlling a first communication interface to synchronize the data account with a plurality of local partner devices, and

wherein each of the plurality of local partner devices is configured to create a distributed data account associated with the individual in a third memory, the distributed data account including the first biometric token and the registration information stored in the data account.

19. The non-transitory computer-readable medium of claim 17, wherein the data account expires after a set period of time, the set of operations further includes

deleting the data account after an expiration of the set period of time, or

permanently disabling the data account after the expiration of the set period of time.

20. The non-transitory computer-readable medium of claim 17, further comprising:

receiving an input from the individual that revokes consent of the individual with respect to the data account;

receiving the second set of the biometrics of the individual;

generating the second biometric token from the second set of the biometrics of the individual that is received;

identifying the individual and the data account by matching the second biometric token that is generated to the first biometric token that is stored in the data account; and

deleting or permanently disabling the data account in response to receiving the input and identifying the data account.

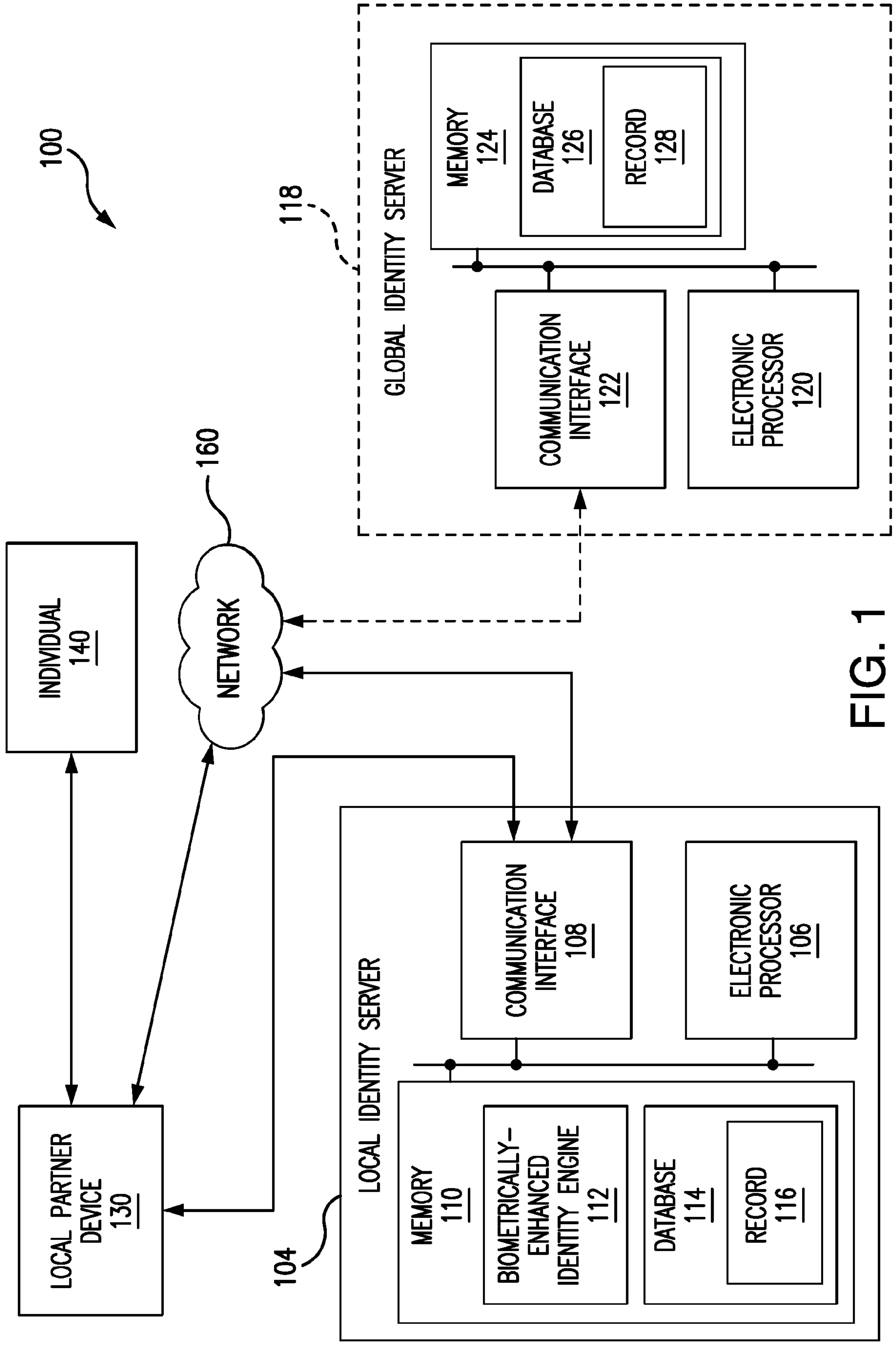

100
INDIVIDUAL 140
NETWORK
160
118
GLOBAL IDENTITY SERVER
MEMORY 124
DATABASE 126
RECORD 128
COMMUNICATION INTERFACE 122
ELECTRONIC PROCESSOR 120
LOCAL PARTNER DEVICE 130
104
LOCAL IDENTITY SERVER
COMMUNICATION INTERFACE 108
ELECTRONIC PROCESSOR 106
MEMORY 110
BIOMETRICALLY-ENHANCED IDENTITY ENGINE 112
DATABASE 114
RECORD 116

FIG. 1

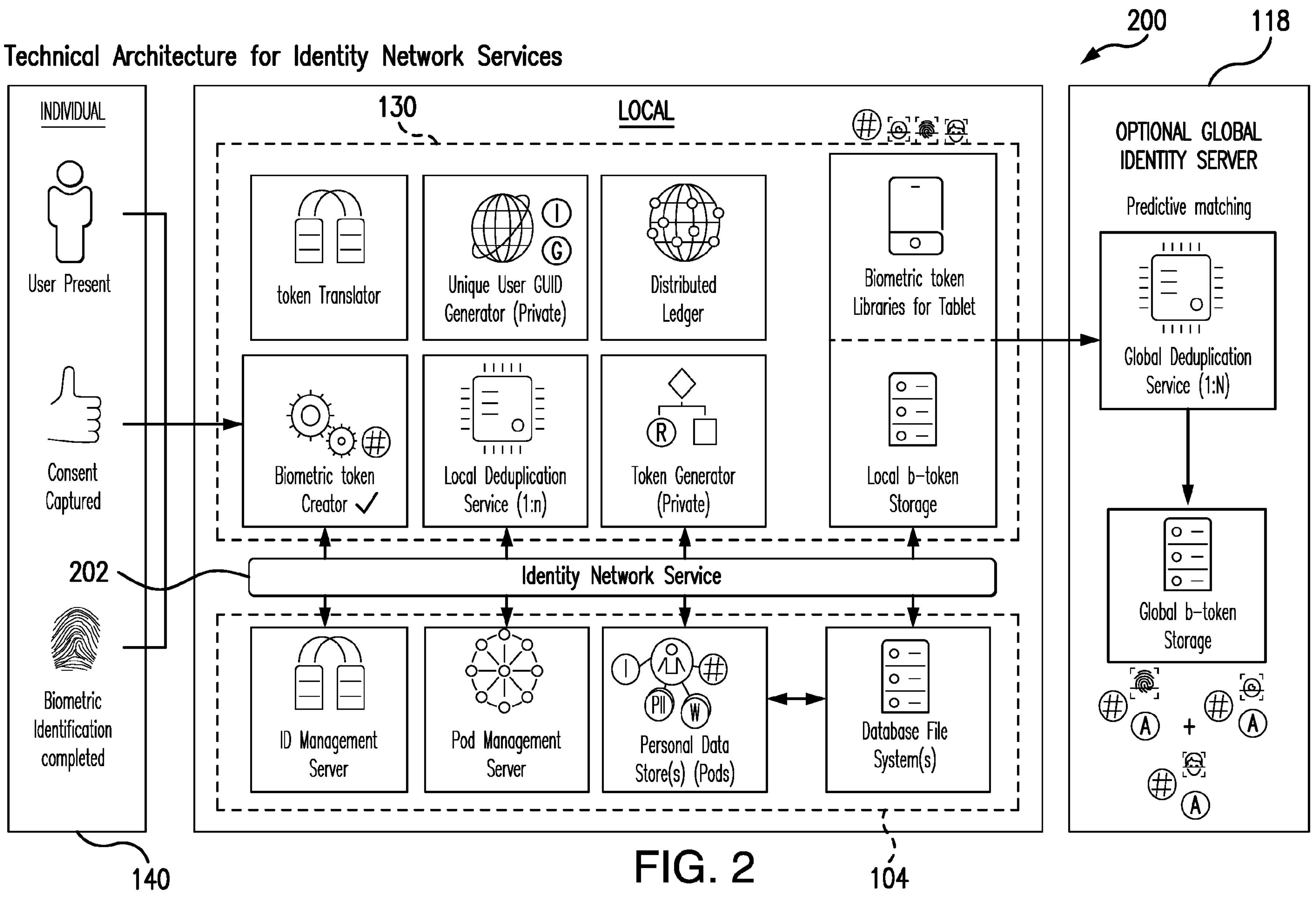

Technical Architecture for Identity Network Services
200
118
INDIVIDUAL
User Present
Consent Captured
202
Biometric Identification completed
140
LOCAL
130
token Translator
Unique User GUID Generator (Private)
I
G
Distributed Ledger
Biometric token Libraries for Tablet
Biometric token Creator ✓
#
Local Deduplication Service (1:n)
Token Generator (Private)
R
Local b-token Storage
#
Identity Network Service
ID Management Server
Pod Management Server
Personal Data Store(s) (Pods)
I
#
PII
W
Database File System(s)
104
OPTIONAL GLOBAL IDENTITY SERVER
Predictive matching
Global Deduplication Service (1:N)
Global b-token Storage
#
A
+
#
A
#
A

FIG. 2

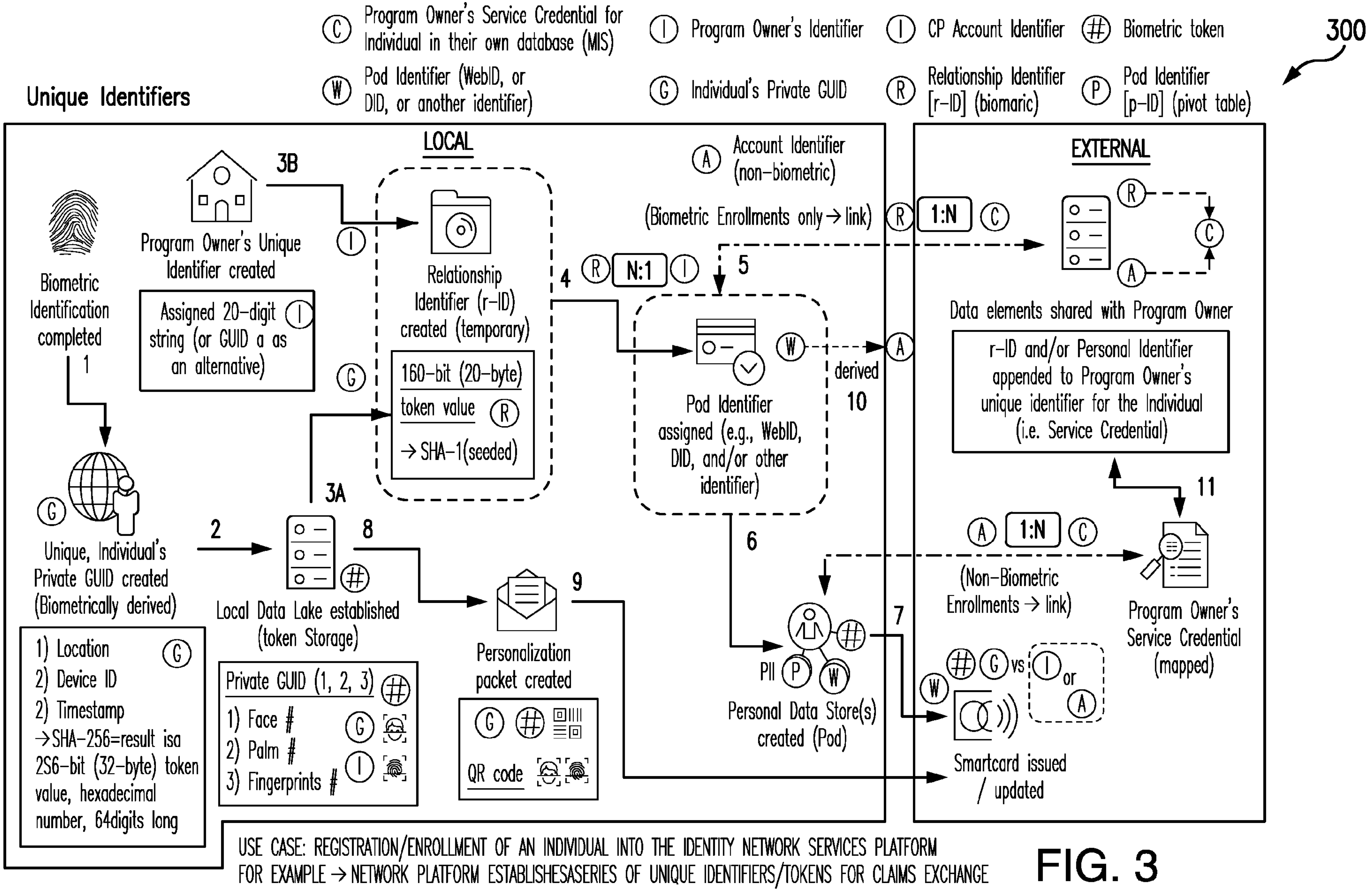

300
Unique Identifiers
C Program Owner's Service Credential for Individual in their own database (MIS)
W Pod Identifier (WebID, or DID, or another identifier)
I Program Owner's Identifier
G Individual's Private GUID
I CP Account Identifier
R Relationship Identifier [r–ID] (biomaric)
# Biometric token
P Pod Identifier [p–ID] (pivot table)
LOCAL
EXTERNAL
Biometric Identification completed
1
Program Owner's Unique Identifier created
Assigned 20–digit string (or GUID a as an alternative) I
3B
I
G
Relationship Identifier (r–ID) created (temporary)
160–bit (20–byte) token value R
→ SHA–1(seeded)
A Account Identifier (non–biometric)
(Biometric Enrollments only → link)
R 1:N C
4
R N:1 I
5
Pod Identifier assigned (e.g., WebID, DID, and/or other identifier)
W
derived
10
A
Data elements shared with Program Owner
r–ID and/or Personal Identifier appended to Program Owner's unique identifier for the Individual (i.e. Service Credential)
11
G
Unique, Individual's Private GUID created (Biometrically derived)
1) Location G
2) Device ID
2) Timestamp
→SHA–256=result isa 2S6–bit (32–byte) token value, hexadecimal number, 64digits long
2
3A
8
#
Local Data Lake established (token Storage)
Private GUID (1, 2, 3) #
1) Face # G
2) Palm #
3) Fingerprints # I
9
Personalization packet created
G #
QR code
6
A 1:N C
(Non–Biometric Enrollments → link)
Program Owner's Service Credential (mapped)
PII P W #
Personal Data Store(s) created (Pod)
7
W # G vs I or A
Smartcard issued / updated
USE CASE: REGISTRATION/ENROLLMENT OF AN INDIVIDUAL INTO THE IDENTITY NETWORK SERVICES PLATFORM
FOR EXAMPLE → NETWORK PLATFORM ESTABLISHESASERIES OF UNIQUE IDENTIFIERS/TOKENS FOR CLAIMS EXCHANGE

FIG. 3

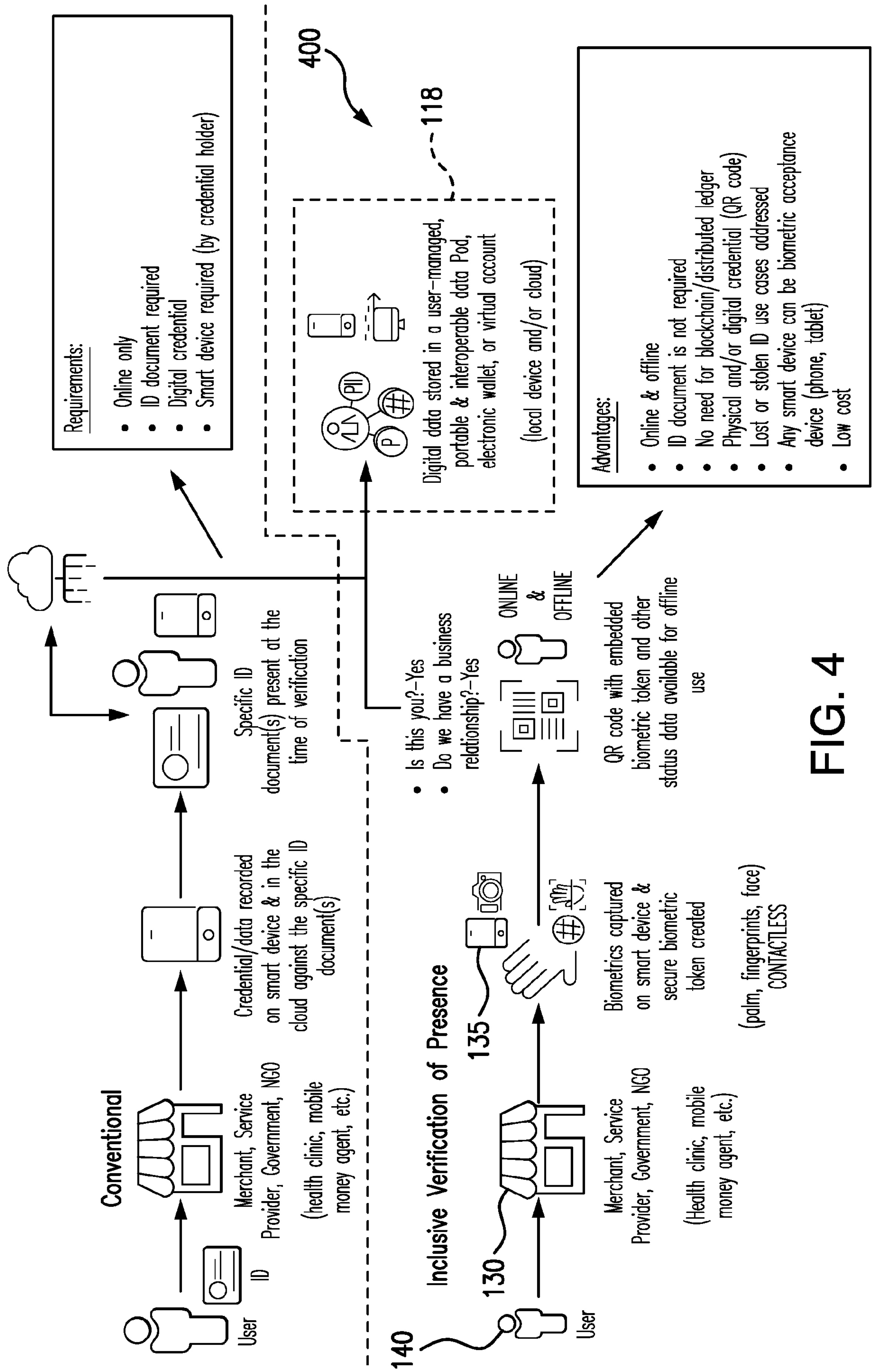

Conventional
User
ID
Merchant, Service Provider, Government, NGO
(health clinic, mobile money agent, etc.)
Credential/data recorded on smart device & in the cloud against the specific ID document(s)
Specific ID document(s) present at the time of verification
Requirements:
• Online only
• ID document required
• Digital credential
• Smart device required (by credential holder)
400
118
PII
P
#
Digital data stored in a user–managed, portable & interoperable data Pod, electronic wallet, or virtual account
(local device and/or cloud)
140
Inclusive Verification of Presence
130
135
User
Merchant, Service Provider, Government, NGO
(Health clinic, mobile money agent, etc.)
#
Biometrics captured on smart device & secure biometric token created
(palm, fingerprints, face) CONTACTLESS
• Is this you?–Yes
• Do we have a business relationship?–Yes
ONLINE & OFFLINE
QR code with embedded biometric token and other status data available for offline use
Advantages:
• Online & offline
• ID document is not required
• No need for blockchain/distributed ledger
• Physical and/or digital credential (QR code)
• Lost or stolen ID use cases addressed
• Any smart device can be biometric acceptance device (phone, tablet)
• Low cost

FIG. 4

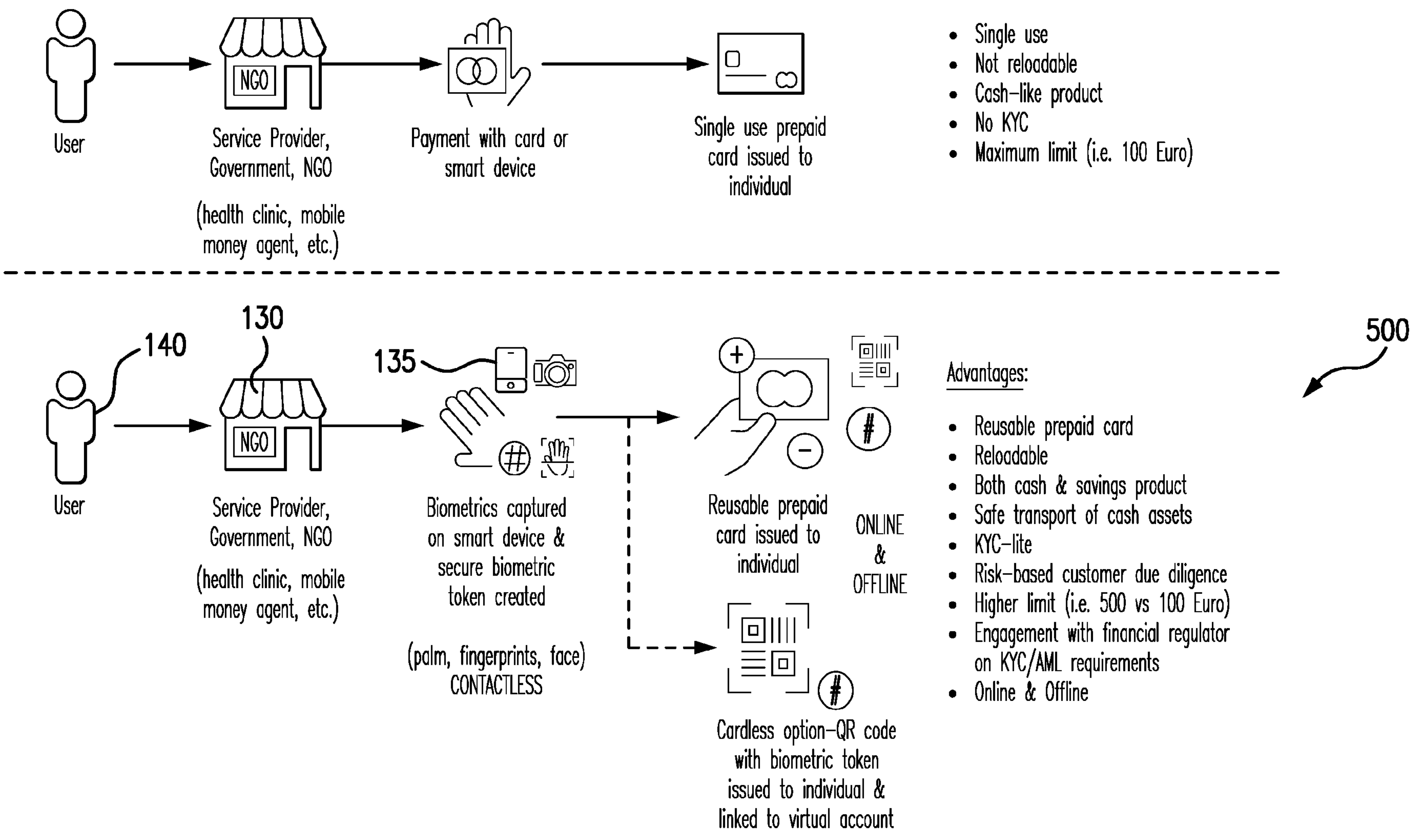

User
Service Provider, Government, NGO
(health clinic, mobile money agent, etc.)
Payment with card or smart device
Single use prepaid card issued to individual
• Single use
• Not reloadable
• Cash-like product
• No KYC
• Maximum limit (i.e. 100 Euro)
500
140
130
135
User
Service Provider, Government, NGO
(health clinic, mobile money agent, etc.)
NGO
Biometrics captured on smart device & secure biometric token created
(palm, fingerprints, face) CONTACTLESS
+
−
#
Reusable prepaid card issued to individual
ONLINE & OFFLINE
Cardless option–QR code with biometric token issued to individual & linked to virtual account
Advantages:
• Reusable prepaid card
• Reloadable
• Both cash & savings product
• Safe transport of cash assets
• KYC-lite
• Risk-based customer due diligence
• Higher limit (i.e. 500 vs 100 Euro)
• Engagement with financial regulator on KYC/AML requirements
• Online & Offline

FIG. 5

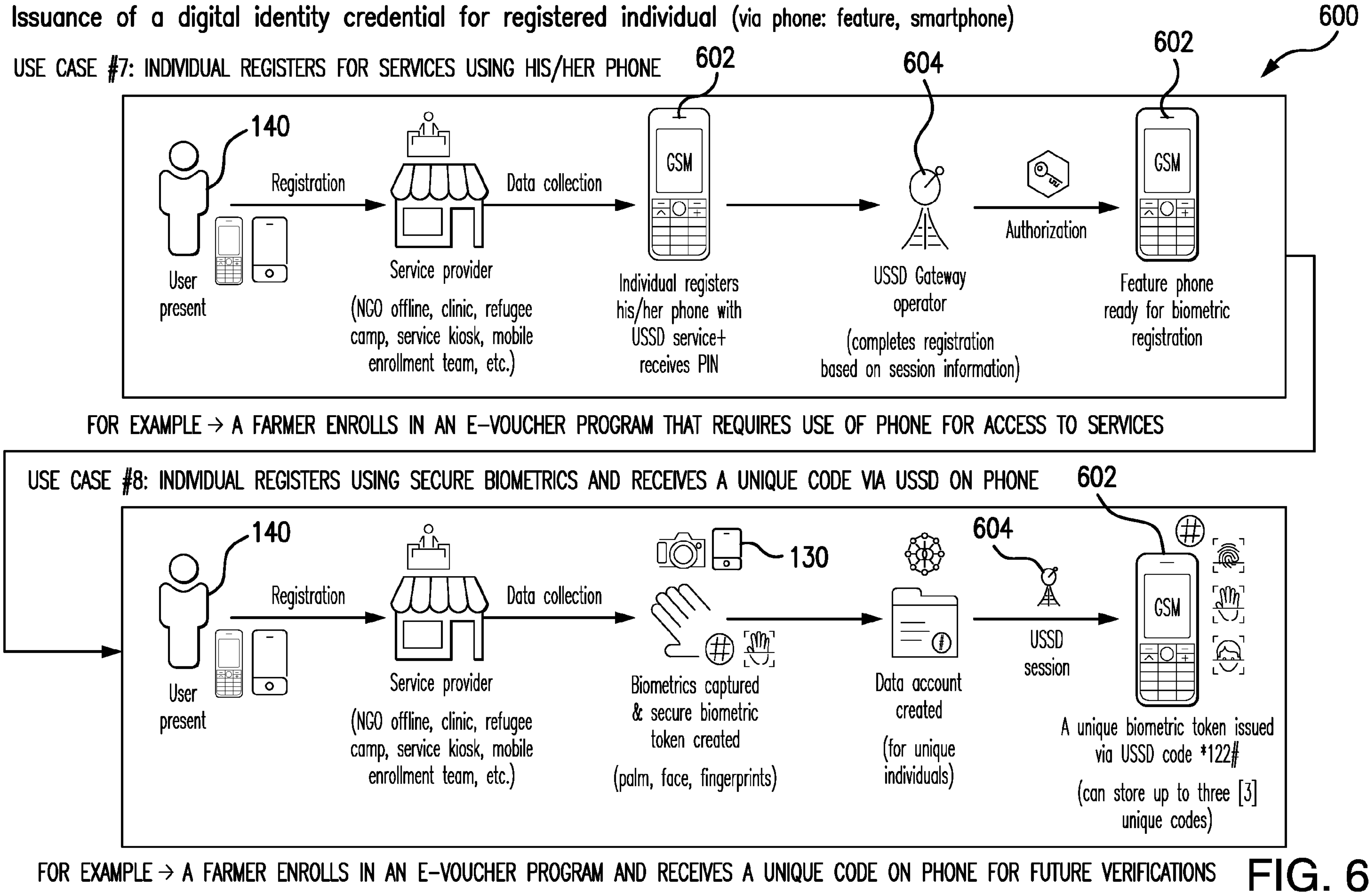

Issuance of a digital identity credential for registered individual (via phone: feature, smartphone)
600
USE CASE #7: INDIVIDUAL REGISTERS FOR SERVICES USING HIS/HER PHONE
602
604
602
140
Registration
Data collection
GSM
Authorization
GSM
User present
Service provider
(NGO offline, clinic, refugee camp, service kiosk, mobile enrollment team, etc.)
Individual registers his/her phone with USSD service+ receives PIN
USSD Gateway operator
(completes registration based on session information)
Feature phone ready for biometric registration
FOR EXAMPLE → A FARMER ENROLLS IN AN E-VOUCHER PROGRAM THAT REQUIRES USE OF PHONE FOR ACCESS TO SERVICES
USE CASE #8: INDIVIDUAL REGISTERS USING SECURE BIOMETRICS AND RECEIVES A UNIQUE CODE VIA USSD ON PHONE
602
140
130
604
Registration
Data collection
USSD session
GSM
User present
Service provider
(NGO offline, clinic, refugee camp, service kiosk, mobile enrollment team, etc.)
Biometrics captured & secure biometric token created
(palm, face, fingerprints)
Data account created
(for unique individuals)
A unique biometric token issued via USSD code *122#
(can store up to three [3] unique codes)
FOR EXAMPLE → A FARMER ENROLLS IN AN E-VOUCHER PROGRAM AND RECEIVES A UNIQUE CODE ON PHONE FOR FUTURE VERIFICATIONS

FIG. 6

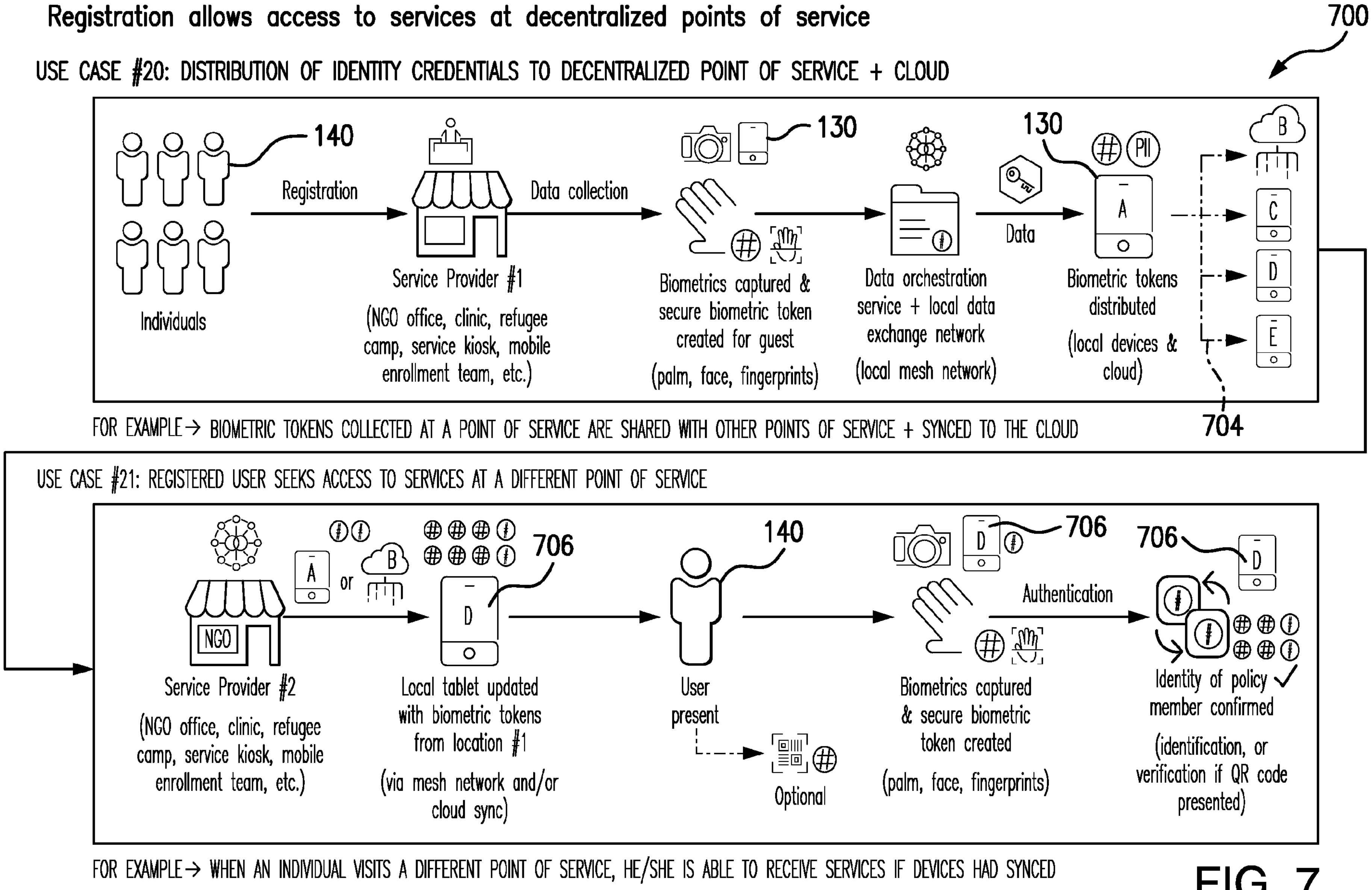

Registration allows access to services at decentralized points of service
700
USE CASE #20: DISTRIBUTION OF IDENTITY CREDENTIALS TO DECENTRALIZED POINT OF SERVICE + CLOUD
140
Individuals
Registration
Service Provider #1
(NGO office, clinic, refugee camp, service kiosk, mobile enrollment team, etc.)
Data collection
130
Biometrics captured & secure biometric token created for guest
(palm, face, fingerprints)
Data orchestration service + local data exchange network
(local mesh network)
Data
130
PII
A
Biometric tokens distributed
(local devices & cloud)
B
C
D
E
704
FOR EXAMPLE→ BIOMETRIC TOKENS COLLECTED AT A POINT OF SERVICE ARE SHARED WITH OTHER POINTS OF SERVICE + SYNCED TO THE CLOUD
USE CASE #21: REGISTERED USER SEEKS ACCESS TO SERVICES AT A DIFFERENT POINT OF SERVICE
NGO
Service Provider #2
(NGO office, clinic, refugee camp, service kiosk, mobile enrollment team, etc.)
A
or
B
D
706
Local tablet updated with biometric tokens from location #1
(via mesh network and/or cloud sync)
140
User present
Optional
D
706
Biometrics captured & secure biometric token created
(palm, face, fingerprints)
Authentication
706
D
Identity of policy member confirmed ✓
(identification, or verification if QR code presented)
FOR EXAMPLE→ WHEN AN INDIVIDUAL VISITS A DIFFERENT POINT OF SERVICE, HE/SHE IS ABLE TO RECEIVE SERVICES IF DEVICES HAD SYNCED

FIG. 7

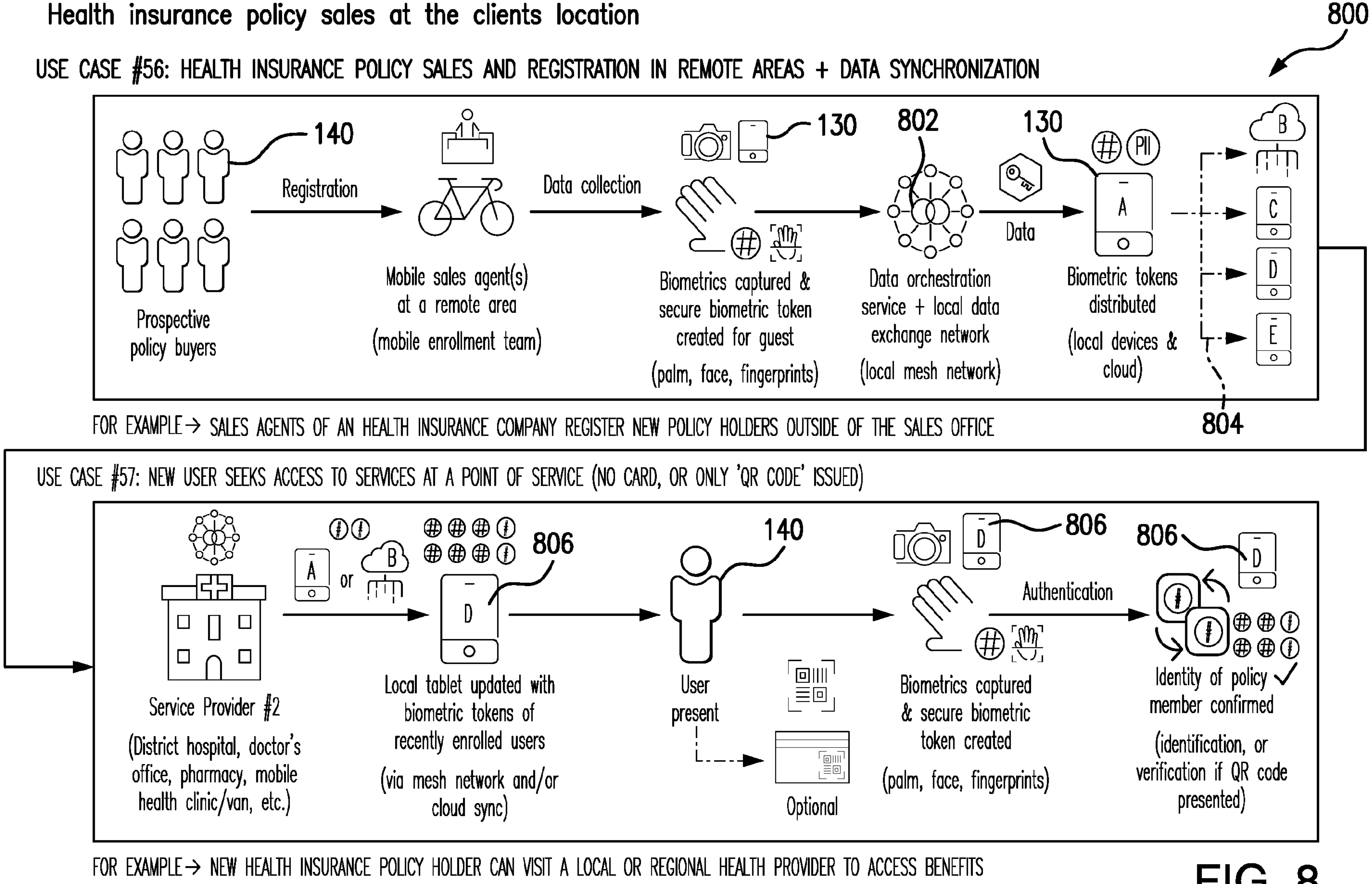

Health insurance policy sales at the clients location
800
USE CASE #56: HEALTH INSURANCE POLICY SALES AND REGISTRATION IN REMOTE AREAS + DATA SYNCHRONIZATION
140
Registration
Prospective policy buyers
Data collection
Mobile sales agent(s) at a remote area
(mobile enrollment team)
130
Biometrics captured & secure biometric token created for guest
(palm, face, fingerprints)
802
Data orchestration service + local data exchange network
(local mesh network)
Data
130
PII
A
Biometric tokens distributed
(local devices & cloud)
B
C
D
E
804
FOR EXAMPLE→ SALES AGENTS OF AN HEALTH INSURANCE COMPANY REGISTER NEW POLICY HOLDERS OUTSIDE OF THE SALES OFFICE
USE CASE #57: NEW USER SEEKS ACCESS TO SERVICES AT A POINT OF SERVICE (NO CARD, OR ONLY 'QR CODE' ISSUED)
Service Provider #2
(District hospital, doctor's office, pharmacy, mobile health clinic/van, etc.)
A
or
B
806
D
Local tablet updated with biometric tokens of recently enrolled users
(via mesh network and/or cloud sync)
140
User present
Optional
D
806
Biometrics captured & secure biometric token created
(palm, face, fingerprints)
Authentication
806
D
Identity of policy member confirmed ✓
(identification, or verification if QR code presented)
FOR EXAMPLE→ NEW HEALTH INSURANCE POLICY HOLDER CAN VISIT A LOCAL OR REGIONAL HEALTH PROVIDER TO ACCESS BENEFITS

FIG. 8

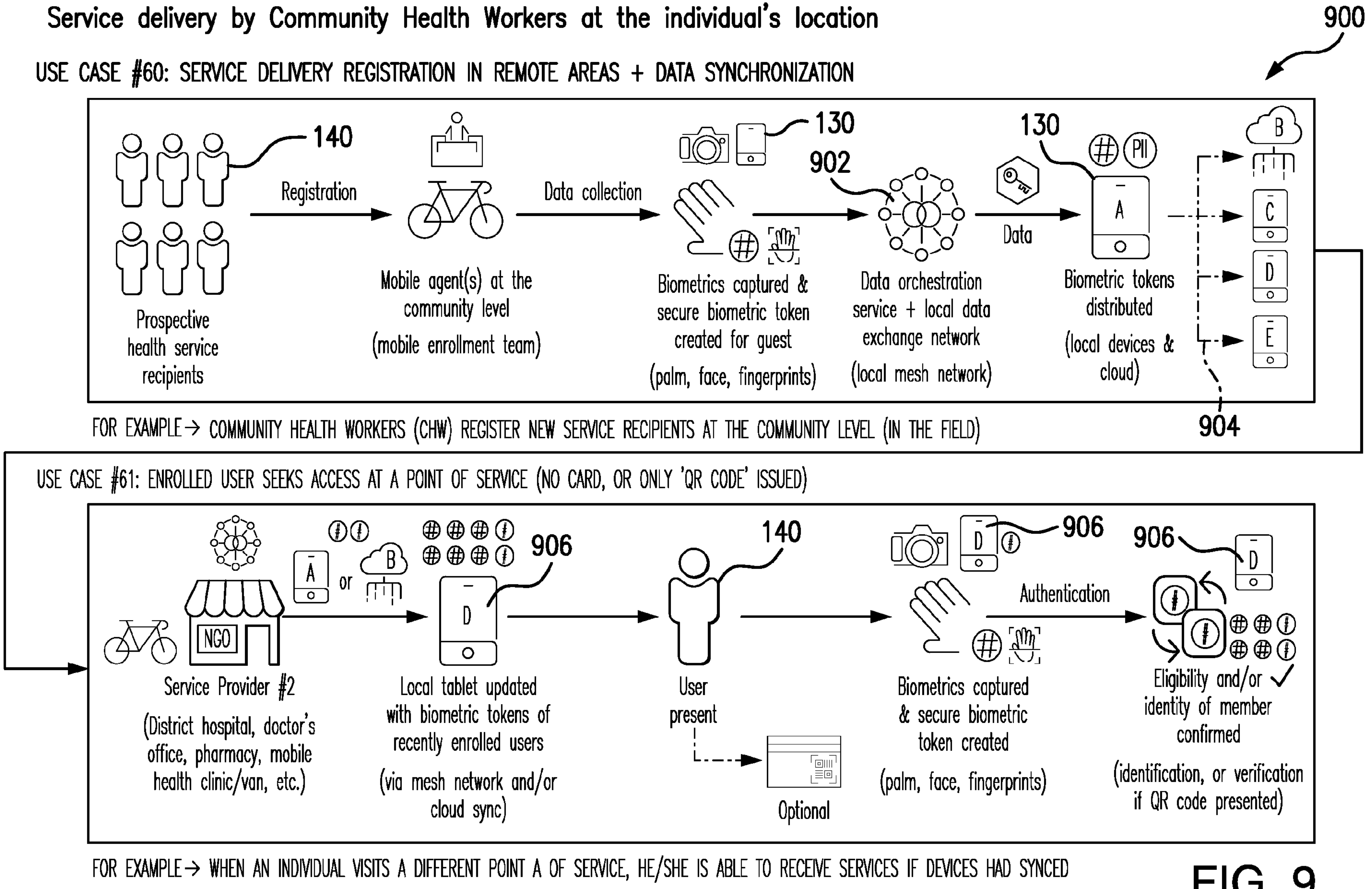
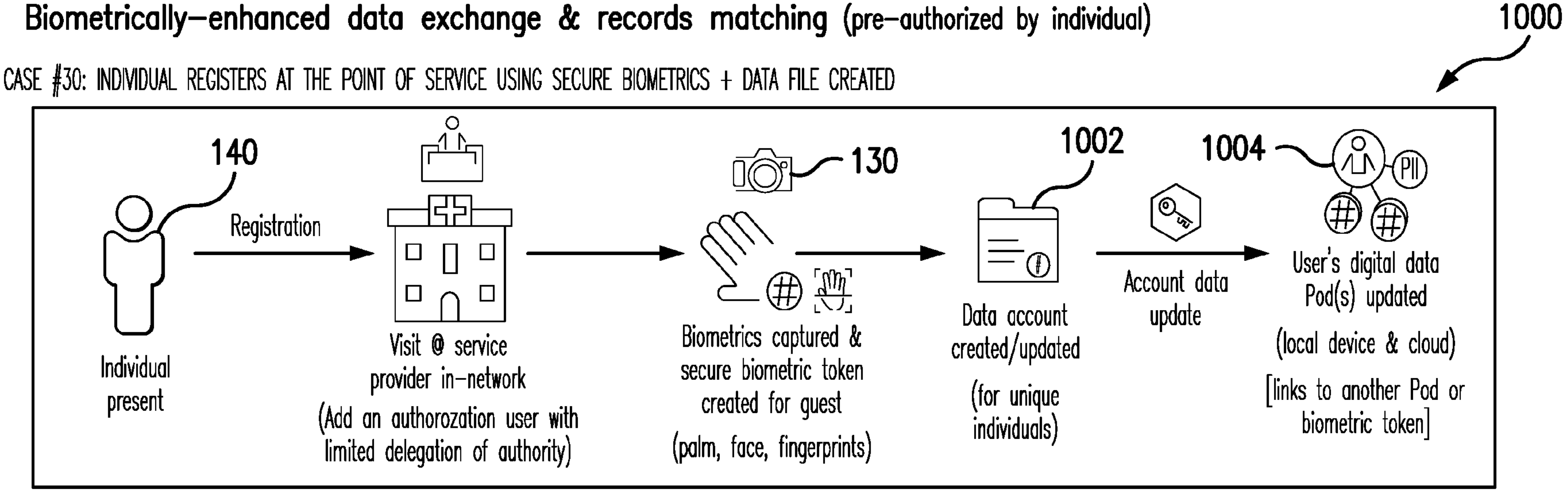

Service delivery by Community Health Workers at the individual's location
900
USE CASE #60: SERVICE DELIVERY REGISTRATION IN REMOTE AREAS + DATA SYNCHRONIZATION
140
Prospective health service recipients
Registration
Mobile agent(s) at the community level
(mobile enrollment team)
Data collection
130
Biometrics captured & secure biometric token created for guest
(palm, face, fingerprints)
902
Data orchestration service + local data exchange network
(local mesh network)
Data
130
PII
A
Biometric tokens distributed
(local devices & cloud)
B
C
D
E
904
FOR EXAMPLE→ COMMUNITY HEALTH WORKERS (CHW) REGISTER NEW SERVICE RECIPIENTS AT THE COMMUNITY LEVEL (IN THE FIELD)
USE CASE #61: ENROLLED USER SEEKS ACCESS AT A POINT OF SERVICE (NO CARD, OR ONLY 'QR CODE' ISSUED)
NGO
Service Provider #2
(District hospital, doctor's office, pharmacy, mobile health clinic/van, etc.)
A
or
B
906
D
Local tablet updated with biometric tokens of recently enrolled users
(via mesh network and/or cloud sync)
140
User present
Optional
D
906
Biometrics captured & secure biometric token created
(palm, face, fingerprints)
Authentication
906
D
Eligibility and/or identity of member confirmed ✓
(identification, or verification if QR code presented)
FOR EXAMPLE→ WHEN AN INDIVIDUAL VISITS A DIFFERENT POINT A OF SERVICE, HE/SHE IS ABLE TO RECEIVE SERVICES IF DEVICES HAD SYNCED

FIG. 9

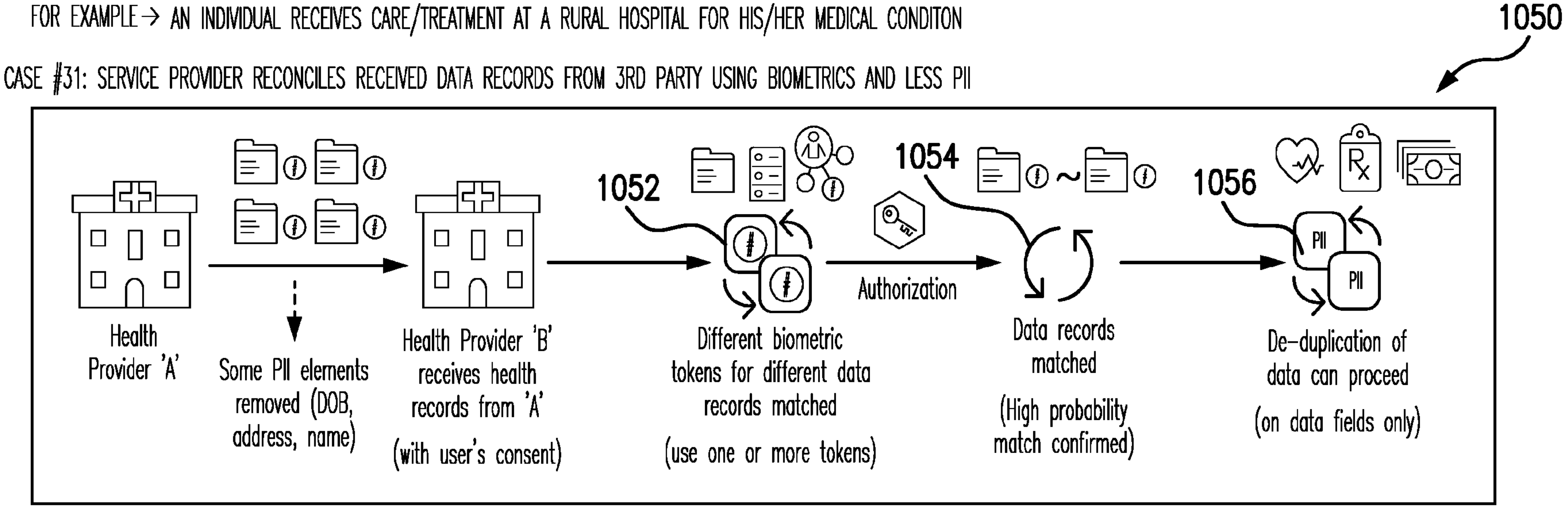
Biometrically-enhanced data exchange & records matching (pre-authorized by individual)

USE CASE #30: INDIVIDUAL REGISTERS AT THE POINT OF SERVICE USING SECURE BIOMETRICS + DATA FILE CREATED


1000
140
Registration
Individual present
Visit @ service provider in-network
(Add an authorozation user with limited delegation of authority)
130
Biometrics captured & secure biometric token created for guest
(palm, face, fingerprints)
1002
Data account created/updated
(for unique individuals)
Account data update
1004
PII
User's digital data Pod(s) updated
(local device & cloud)
[links to another Pod or biometric token]

FOR EXAMPLE→ AN INDIVIDUAL RECEIVES CARE/TREATMENT AT A RURAL HOSPITAL FOR HIS/HER MEDICAL CONDITON

USE CASE #31: SERVICE PROVIDER RECONCILES RECEIVED DATA RECORDS FROM 3RD PARTY USING BIOMETRICS AND LESS PII


1050
Health Provider 'A'
Some PII elements removed (DOB, address, name)
Health Provider 'B' receives health records from 'A'
(with user's consent)
1052
Different biometric tokens for different data records matched
(use one or more tokens)
Authorization
1054
Data records matched
(High probability match confirmed)
1056
Rx
PII
PII
De-duplication of data can proceed
(on data fields only)

FOR EXAMPLE→ A DIFFERENT SPECIALIST OR POINT OF CARE (I.E. REGIONAL HOSPITAL OR DIFFERENT DOCTOR) SEEKS INFO ON PATIENT

FIG. 10

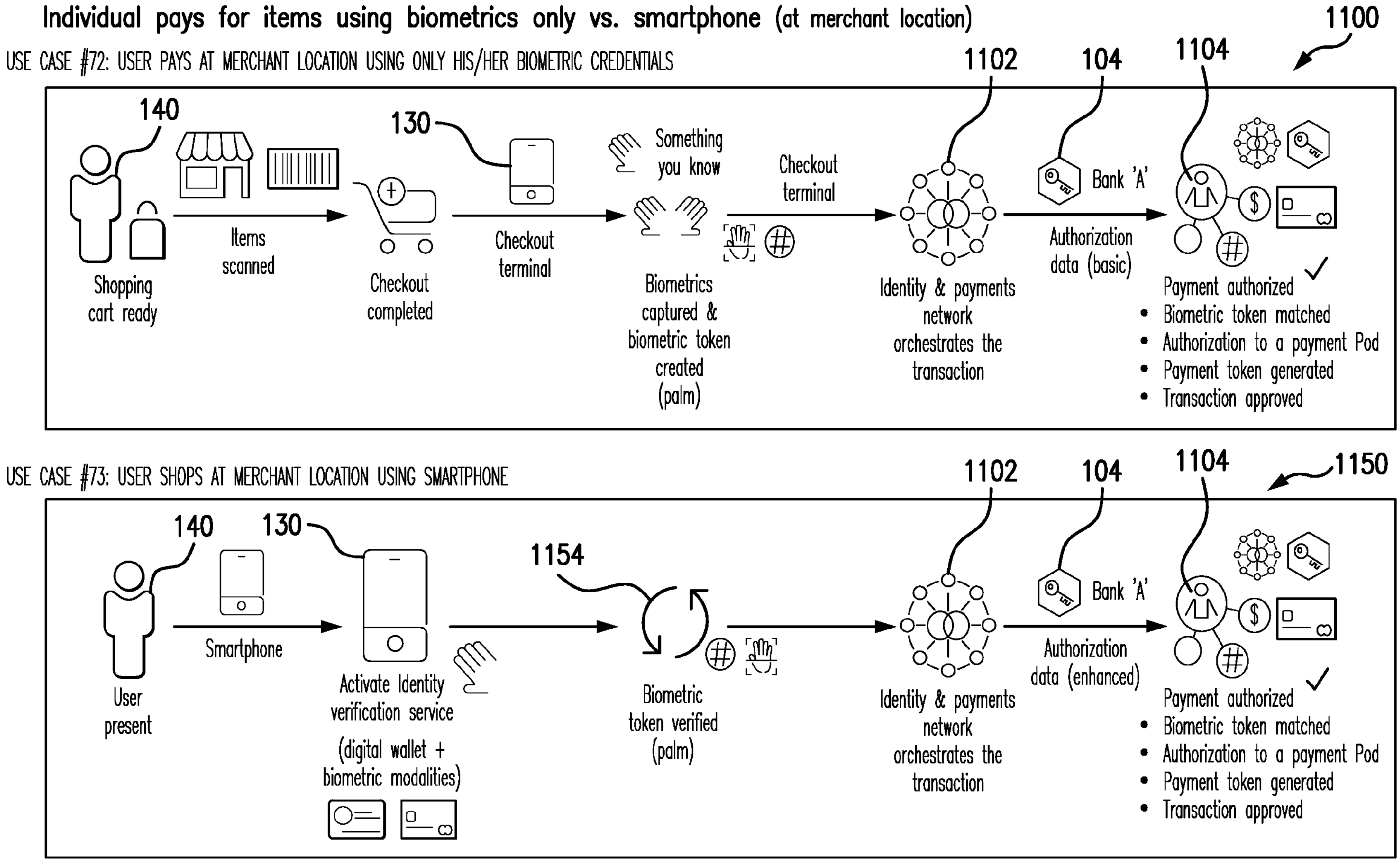

Individual pays for items using biometrics only vs. smartphone (at merchant location)
1100
USE CASE #72: USER PAYS AT MERCHANT LOCATION USING ONLY HIS/HER BIOMETRIC CREDENTIALS
140
Shopping cart ready
Items scanned
Checkout completed
130
Checkout terminal
Something you know
Biometrics captured & biometric token created (palm)
Checkout terminal
1102
Identity & payments network orchestrates the transaction
104
Bank 'A'
Authorization data (basic)
1104
Payment authorized
• Biometric token matched
• Authorization to a payment Pod
• Payment token generated
• Transaction approved
USE CASE #73: USER SHOPS AT MERCHANT LOCATION USING SMARTPHONE
1150
140
User present
Smartphone
130
Activate Identity verification service (digital wallet + biometric modalities)
1154
Biometric token verified (palm)
1102
Identity & payments network orchestrates the transaction
104
Bank 'A'
Authorization data (enhanced)
1104
Payment authorized
• Biometric token matched
• Authorization to a payment Pod
• Payment token generated
• Transaction approved

FIG. 11

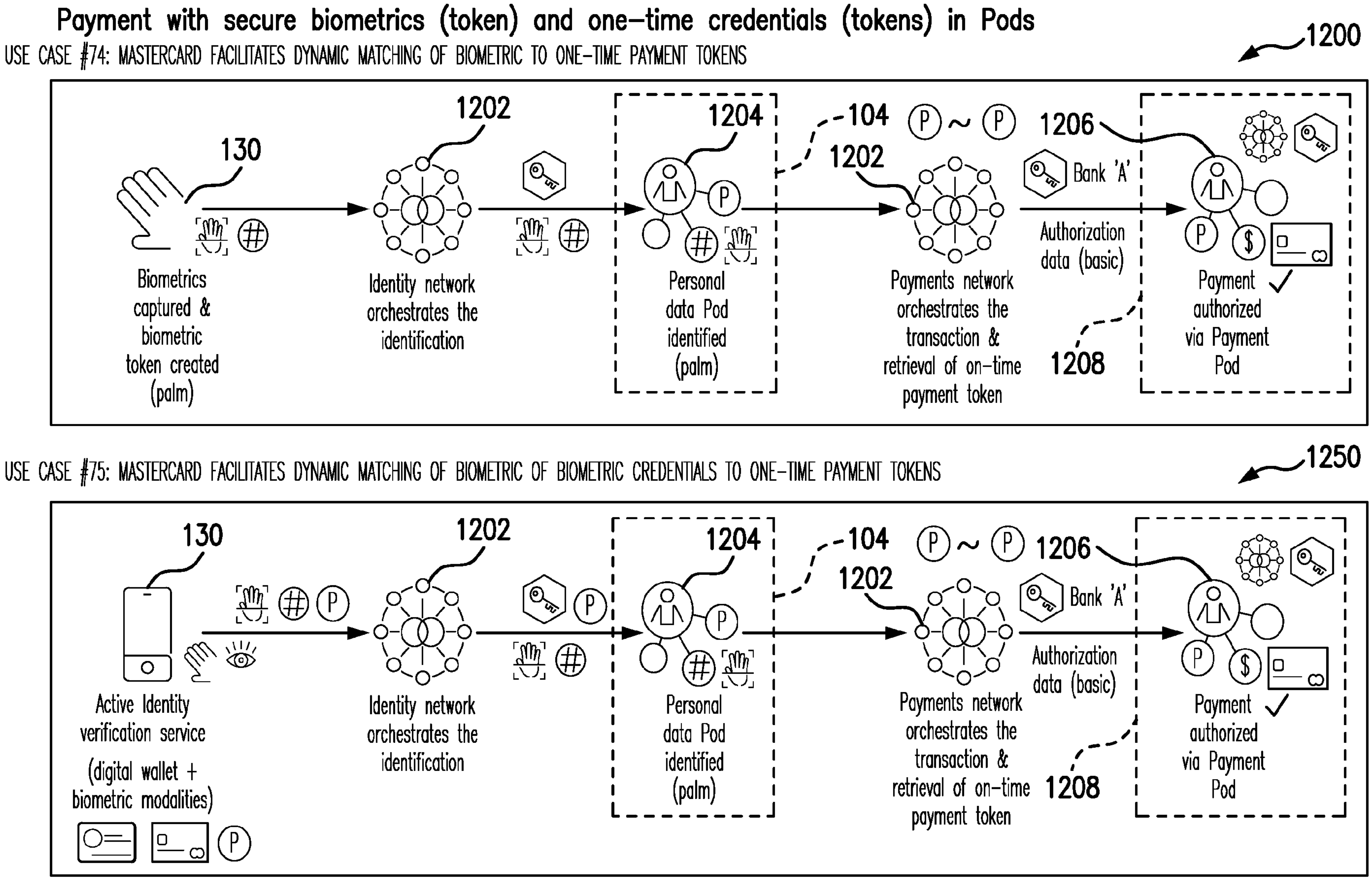

Payment with secure biometrics (token) and one–time credentials (tokens) in Pods
USE CASE #74: MASTERCARD FACILITATES DYNAMIC MATCHING OF BIOMETRIC TO ONE–TIME PAYMENT TOKENS
1200
130
Biometrics captured & biometric token created (palm)
1202
Identity network orchestrates the identification
1204
Personal data Pod identified (palm)
104
1202
P ~ P
Payments network orchestrates the transaction & retrieval of on–time payment token
1206
Bank 'A'
Authorization data (basic)
1208
Payment authorized via Payment Pod
USE CASE #75: MASTERCARD FACILITATES DYNAMIC MATCHING OF BIOMETRIC OF BIOMETRIC CREDENTIALS TO ONE–TIME PAYMENT TOKENS
1250
130
Active Identity verification service
(digital wallet + biometric modalities)
1202
Identity network orchestrates the identification
1204
Personal data Pod identified (palm)
104
1202
P ~ P
Payments network orchestrates the transaction & retrieval of on–time payment token
1206
Bank 'A'
Authorization data (basic)
1208
Payment authorized via Payment Pod

FIG. 12

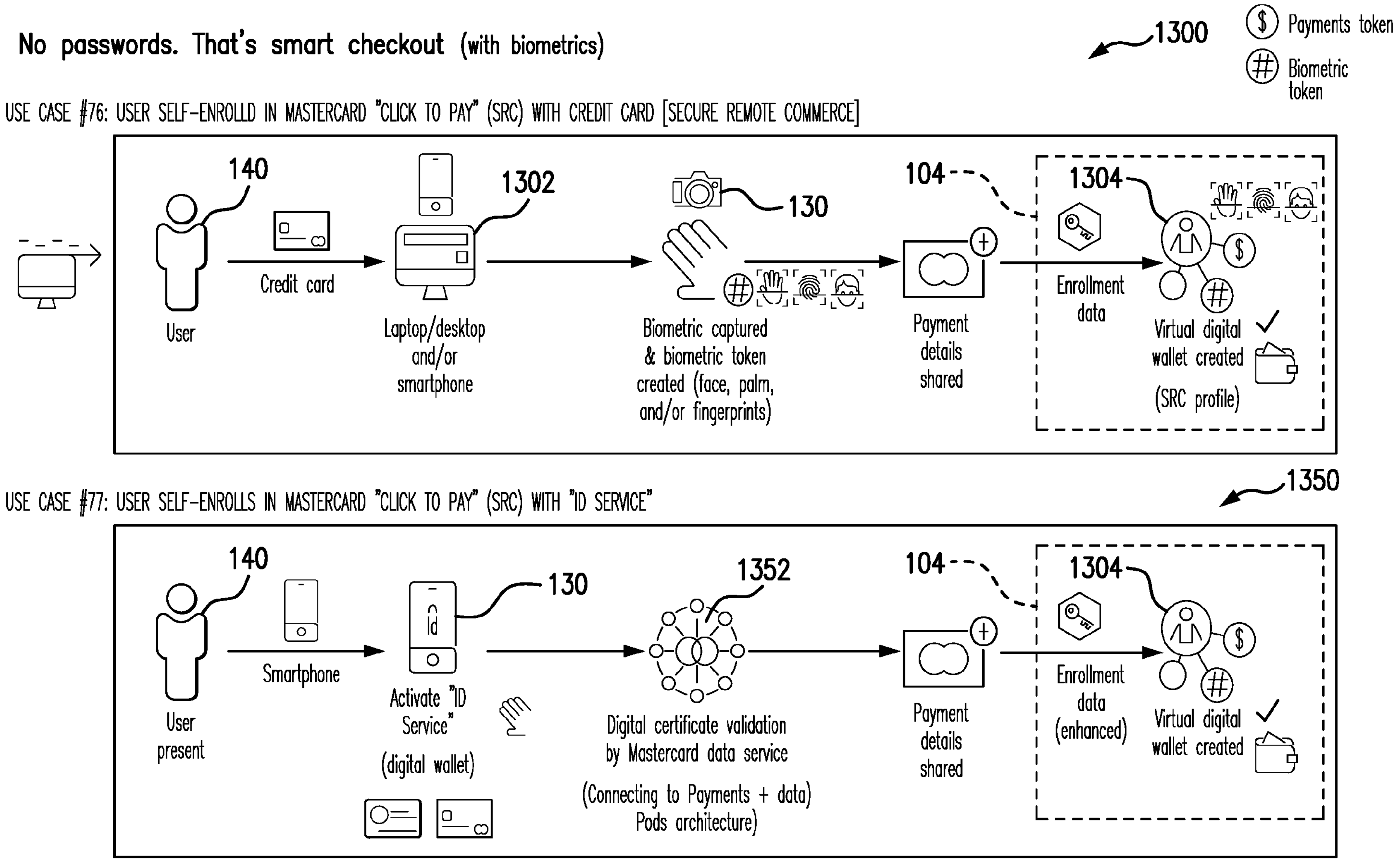

No passwords. That's smart checkout (with biometrics)
1300
$ Payments token
# Biometric token
USE CASE #76: USER SELF-ENROLLD IN MASTERCARD "CLICK TO PAY" (SRC) WITH CREDIT CARD [SECURE REMOTE COMMERCE]
140
User
Credit card
1302
Laptop/desktop and/or smartphone
130
Biometric captured & biometric token created (face, palm, and/or fingerprints)
104
Payment details shared
1304
Enrollment data
Virtual digital wallet created
(SRC profile)
1350
USE CASE #77: USER SELF-ENROLLS IN MASTERCARD "CLICK TO PAY" (SRC) WITH "ID SERVICE"
140
User present
Smartphone
130
Activate "ID Service"
(digital wallet)
1352
Digital certificate validation by Mastercard data service
(Connecting to Payments + data) Pods architecture)
104
Payment details shared
1304
Enrollment data (enhanced)
Virtual digital wallet created

FIG. 13

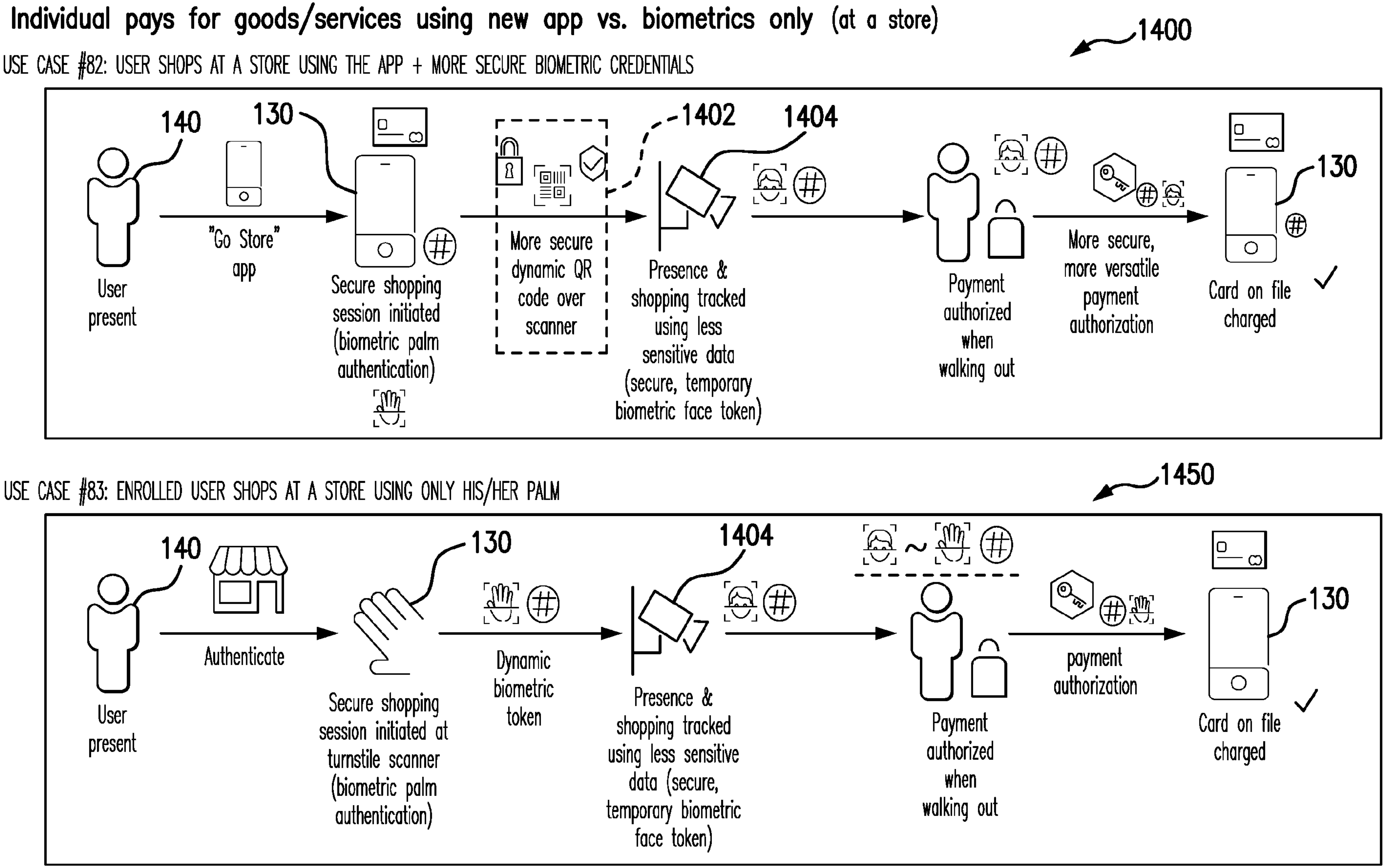

Individual pays for goods/services using new app vs. biometrics only (at a store)
1400
USE CASE #82: USER SHOPS AT A STORE USING THE APP + MORE SECURE BIOMETRIC CREDENTIALS
140
130
User present
"Go Store" app
Secure shopping session initiated (biometric palm authentication)
More secure dynamic QR code over scanner
1402
1404
Presence & shopping tracked using less sensitive data (secure, temporary biometric face token)
Payment authorized when walking out
More secure, more versatile payment authorization
130
Card on file charged
1450
USE CASE #83: ENROLLED USER SHOPS AT A STORE USING ONLY HIS/HER PALM
140
User present
Authenticate
130
Secure shopping session initiated at turnstile scanner (biometric palm authentication)
Dynamic biometric token
1404
Presence & shopping tracked using less sensitive data (secure, temporary biometric face token)
Payment authorized when walking out
payment authorization
130
Card on file charged

FIG. 14

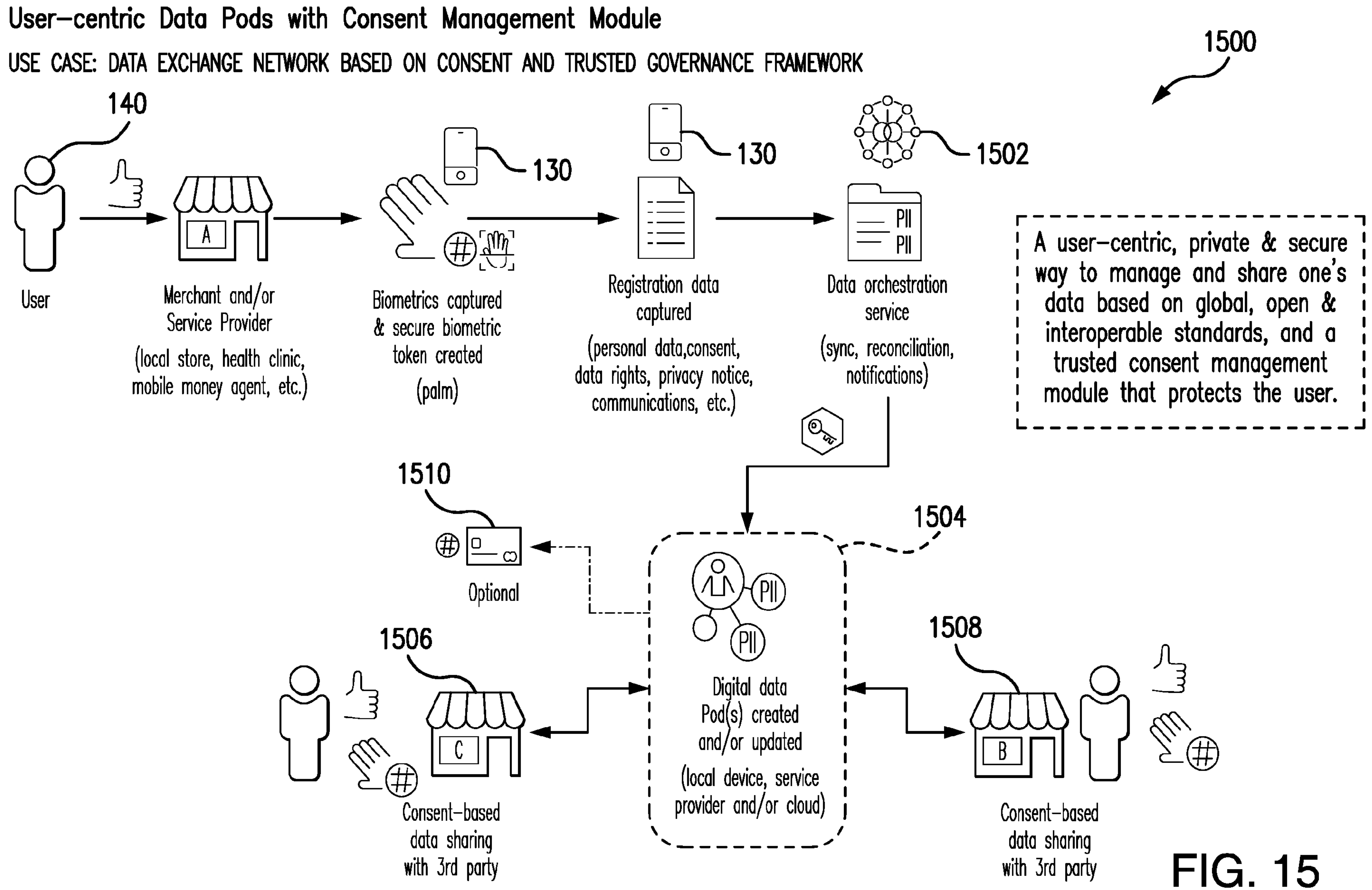
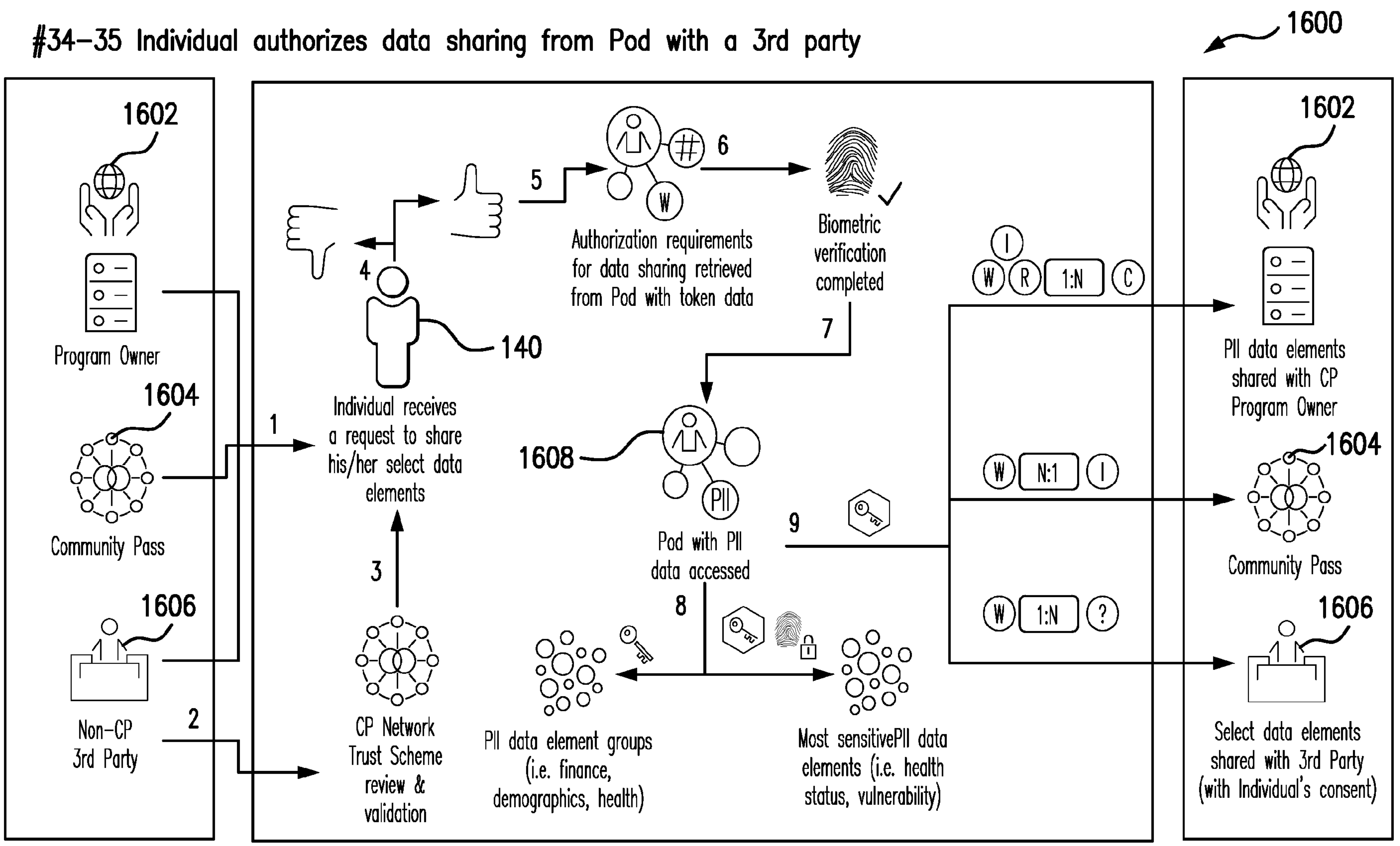
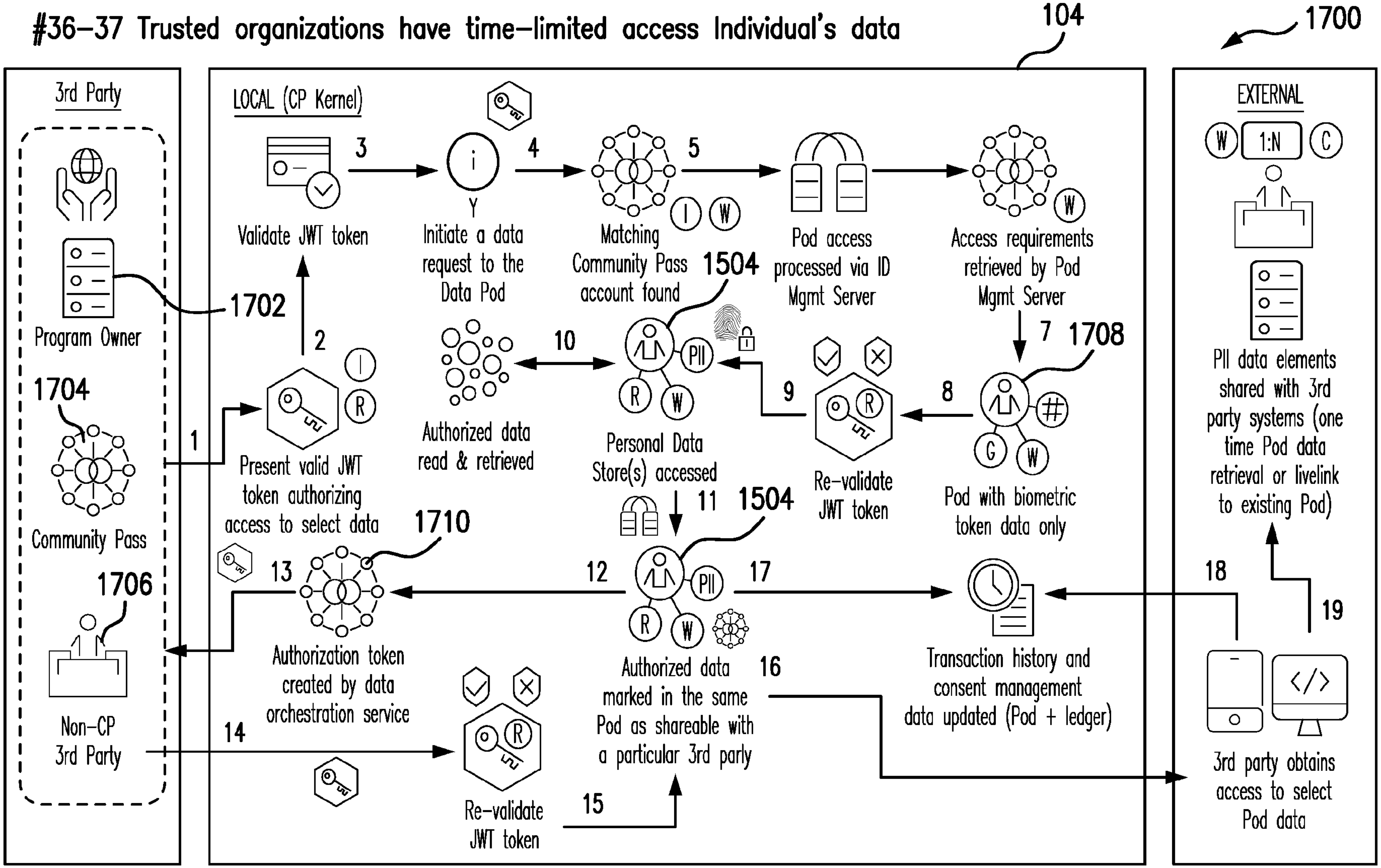

User–centric Data Pods with Consent Management Module
USE CASE: DATA EXCHANGE NETWORK BASED ON CONSENT AND TRUSTED GOVERNANCE FRAMEWORK
1500
140
User
A
Merchant and/or Service Provider
(local store, health clinic, mobile money agent, etc.)
130
#
Biometrics captured & secure biometric token created
(palm)
130
Registration data captured
(personal data,consent, data rights, privacy notice, communications, etc.)
1502
PII
PII
Data orchestration service
(sync, reconciliation, notifications)
A user–centric, private & secure way to manage and share one's data based on global, open & interoperable standards, and a trusted consent management module that protects the user.
1510
#
Optional
1504
PII
PII
Digital data Pod(s) created and/or updated
(local device, service provider and/or cloud)
1506
C
#
Consent–based data sharing with 3rd party
1508
B
#
Consent–based data sharing with 3rd party

FIG. 15



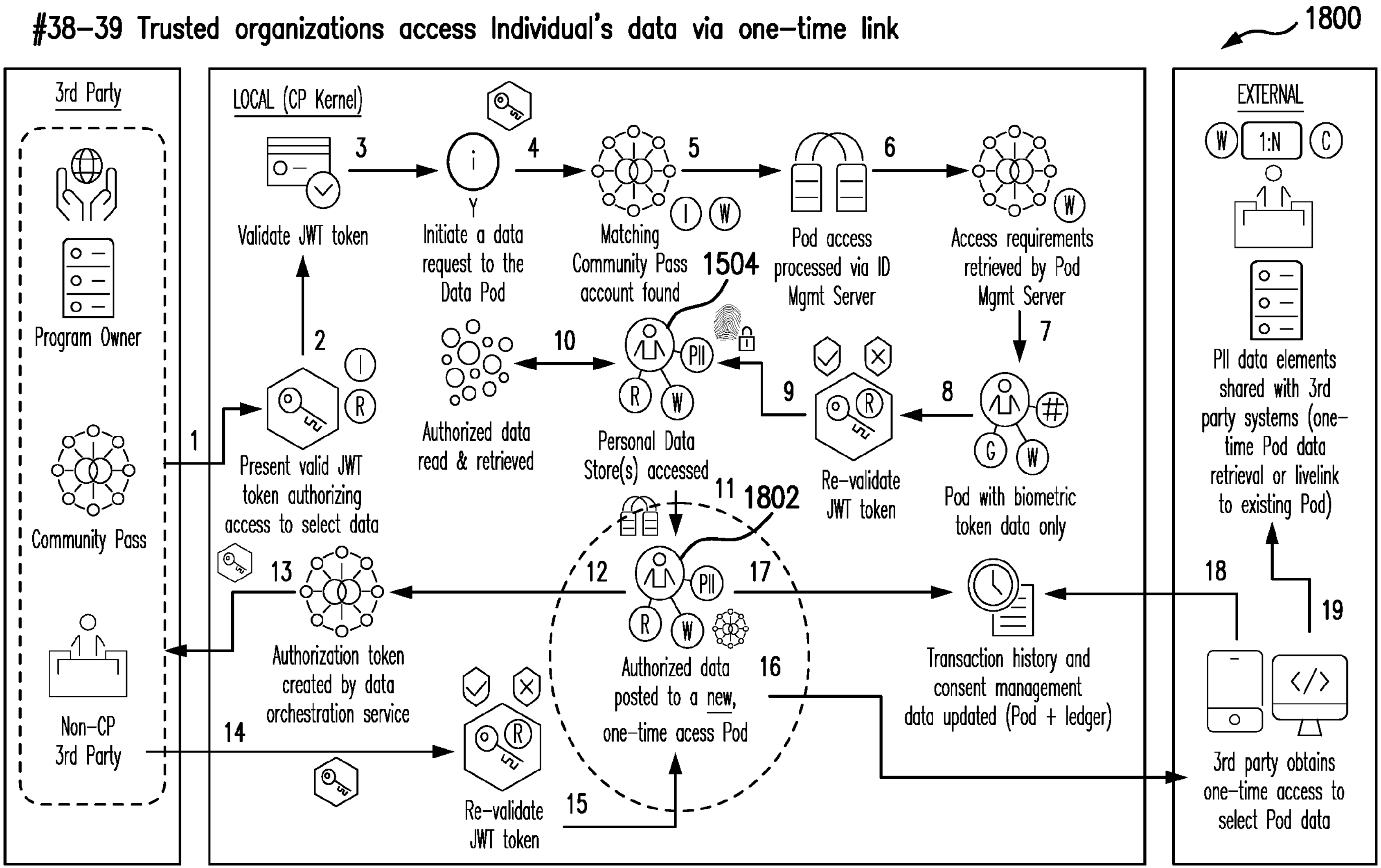
USE CASE: PROCESS AND DATA FLOWS FOR SHARING DATA FROM A PERSONAL DATA STORE (POD)
FOR EXAMPLE →A BENEFICIARY AUTHORIZES DATA SHARING WITH A 3RD PARTY (E.G. MICROFINANCE INSTITUTION)

FIG. 16


#36–37 Trusted organizations have time–limited access Individual's data
1700
104
3rd Party
Program Owner
1702
1704
Community Pass
1706
Non–CP
3rd Party
LOCAL (CP Kernel)
1
2
Present valid JWT token authorizing access to select data
I
R
3
Validate JWT token
4
i
Y
Initiate a data request to the Data Pod
5
I
W
Matching Community Pass account found
1504
Pod access processed via ID Mgmt Server
W
Access requirements retrieved by Pod Mgmt Server
7
1708
#
G
W
Pod with biometric token data only
8
Re–validate JWT token
9
PII
R
W
10
Authorized data read & retrieved
Personal Data Store(s) accessed
11
1504
PII
R
W
12
17
1710
13
Authorization token created by data orchestration service
14
Re–validate JWT token
R
15
Authorized data marked in the same Pod as shareable with a particular 3rd parly
16
Transaction history and consent management data updated (Pod + ledger)
EXTERNAL
W
1:N
C
PII data elements shared with 3rd party systems (one time Pod data retrieval or livelink to existing Pod)
18
19
&lt;/&gt;
3rd party obtains access to select Pod data

USE CASE: 3RD PARTY CAN ACCESS INDIVIDUAL'S DATA FROM HIS/HER POD ON AN ONGOING BASIS
FOR EXAMPLE → NGO CAN ACCESS INDIVIDUAL'S DATA TO GET A FULL PICTURE OF THE BENEFICIARY ANY TIME

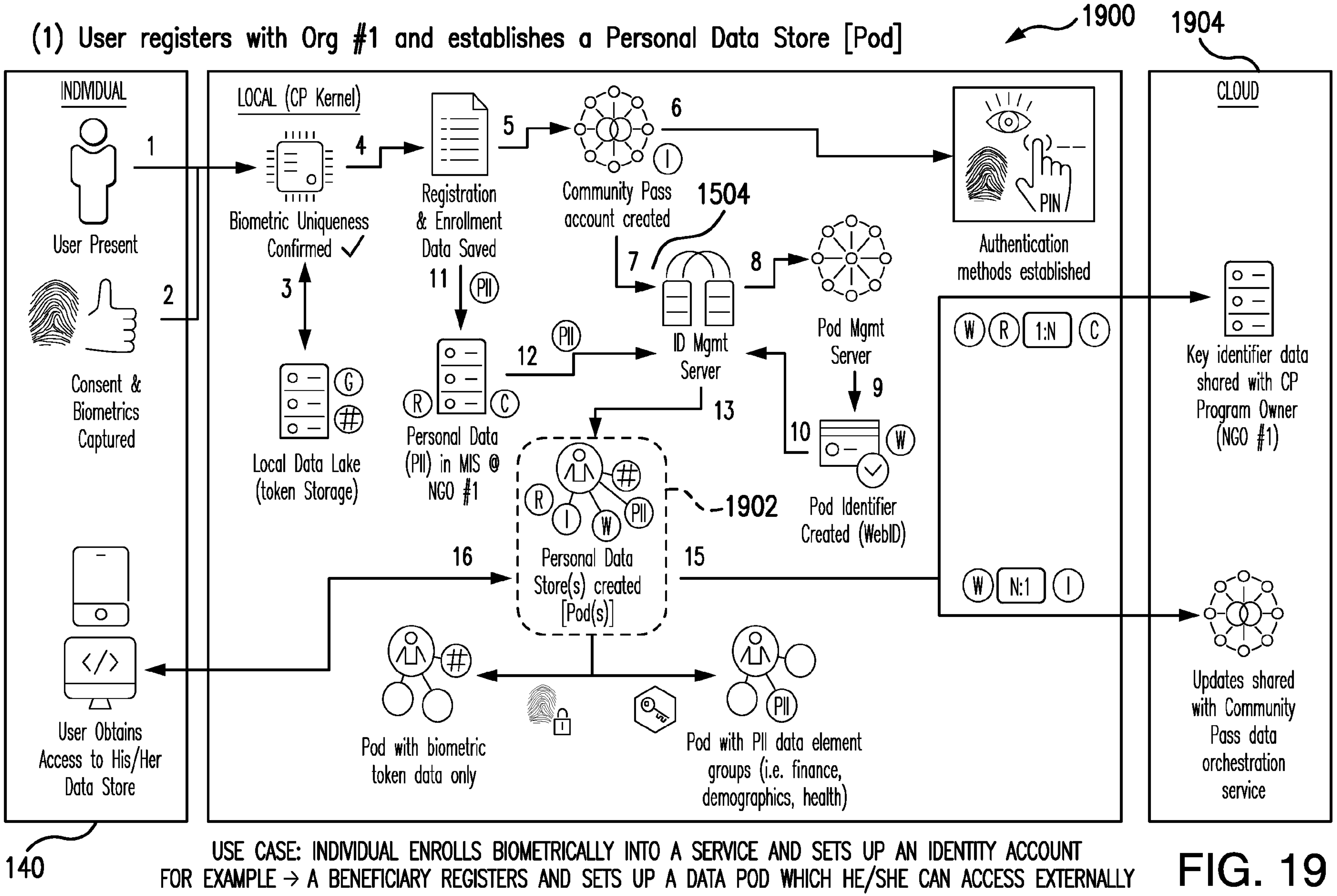
FIG. 17


#38–39 Trusted organizations access Individual's data via one–time link
1800
3rd Party
Program Owner
Community Pass
Non–CP
3rd Party
LOCAL (CP Kernel)
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Validate JWT token
Initiate a data request to the Data Pod
Y
Matching Community Pass account found
1504
Pod access processed via ID Mgmt Server
Access requirements retrieved by Pod Mgmt Server
Present valid JWT token authorizing access to select data
Authorized data read & retrieved
Personal Data Store(s) accessed
Re–validate JWT token
Pod with biometric token data only
1802
Authorization token created by data orchestration service
Authorized data posted to a new, one–time acess Pod
Transaction history and consent management data updated (Pod + ledger)
Re–validate JWT token
I
W
R
PII
G
#
EXTERNAL
W
1:N
C
PII data elements shared with 3rd party systems (one–time Pod data retrieval or livelink to existing Pod)
3rd party obtains one–time access to select Pod data

USE CASE: 3RD PARTY CAN ACCESS INDIVIDUAL'S DATA FROM HIS/HER POD AS ONE–TIME ACTION
FOR EXAMPLE → MICROFINANCE INSTITUTION GETS ACCESS TO SELECT DATA AS PART OF A NEW LOAN APPLICATION

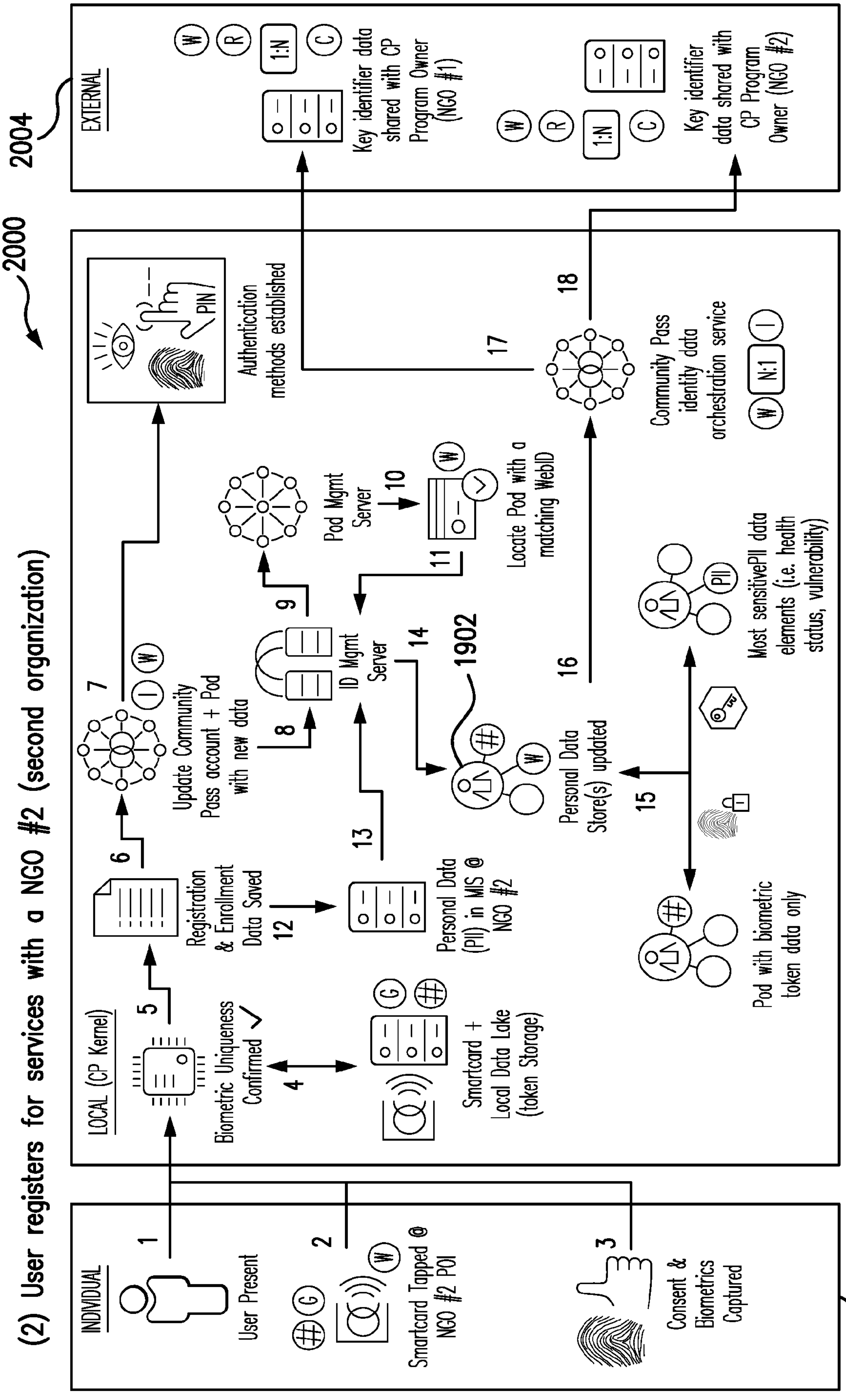
FIG. 18

(1) User registers with Org #1 and establishes a Personal Data Store [Pod]


1900
1904
INDIVIDUAL
User Present
1
2
Consent & Biometrics Captured
User Obtains Access to His/Her Data Store
140
LOCAL (CP Kernel)
Biometric Uniqueness Confirmed ✓
3
Local Data Lake (token Storage)
G
#
4
Registration & Enrollment Data Saved
11
PII
Personal Data (PII) in MIS @ NGO #1
R
C
12
PII
5
6
I
Community Pass account created
1504
7
ID Mgmt Server
8
Pod Mgmt Server
9
10
W
Pod Identifier Created (WebID)
13
R
I
W
PII
#
Personal Data Store(s) created [Pod(s)]
1902
15
16
Pod with biometric token data only
Pod with PII data element groups (i.e. finance, demographics, health)
PIN
Authentication methods established
W
R
1:N
C
W
N:1
I
CLOUD
Key identifier data shared with CP Program Owner (NGO #1)
Updates shared with Community Pass data orchestration service

USE CASE: INDIVIDUAL ENROLLS BIOMETRICALLY INTO A SERVICE AND SETS UP AN IDENTITY ACCOUNT FOR EXAMPLE → A BENEFICIARY REGISTERS AND SETS UP A DATA POD WHICH HE/SHE CAN ACCESS EXTERNALLY

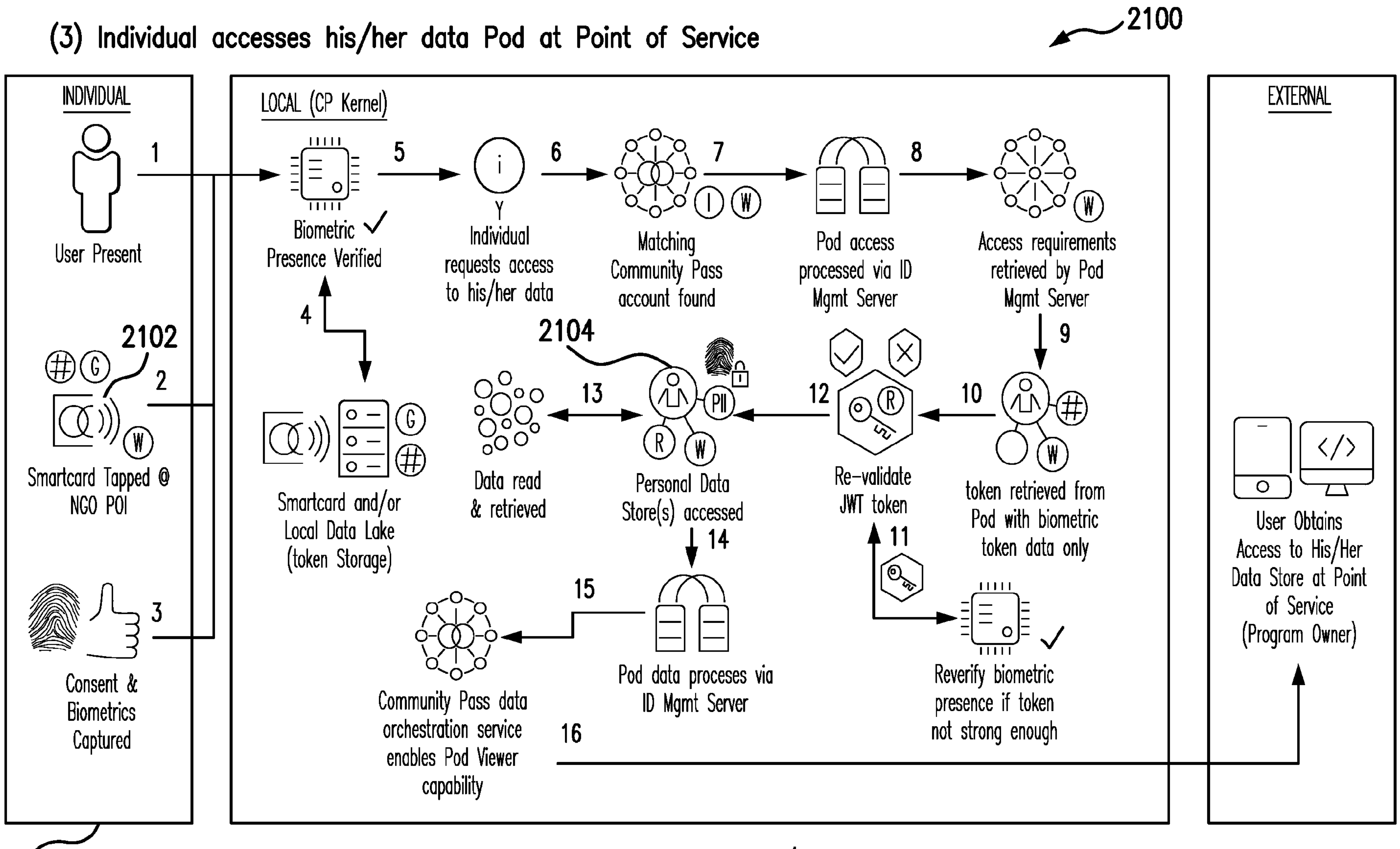
FIG. 19


(2) User registers for services with a NGO #2 (second organization)
2000
2004
140
INDIVIDUAL
1
User Present
2
Smartcard Tapped @ NGO #2 POI
W
G
#
3
Consent & Biometrics Captured
LOCAL (CP Kernel)
Biometric Uniqueness Confirmed ✓
4
Smartcard + Local Data Lake (token Storage)
G
#
5
Registration & Enrollment Data Saved
12
Personal Data (PII) in MIS @ NGO #2
6
7
Update Community Pass account + Pod with new data
I
W
13
8
ID Mgmt Server
9
Pod Mgmt Server
10
11
Locate Pod with a matching WebID
W
14
1902
#
W
Personal Data Store(s) updated
15
Pod with biometric token data only
#
Most sensitivePII data elements (i.e. health status, vulnerability)
PII
16
Authentication methods established
PIN
17
18
Community Pass identity data orchestration service
W
N:1
I
EXTERNAL
Key identifier data shared with CP Program Owner (NGO #1)
W
R
1:N
C
Key identifier data shared with CP Program Owner (NGO #2)
W
R
1:N
C

USE CASE: INDIVIDUAL VISITS ANOTHER NETWORK ORGANIZATION TO REGISTER FOR SERVICES FOR EXAMPLE → A BENEFICIARY EFFICIENTLY REGISTERSTS RECEIVE BENEFITS FROM A 2ND ORGANIZATION

FIG. 20

(3) Individual accesses his/her data Pod at Point of Service


2100
INDIVIDUAL
User Present
1
2102
2
Smartcard Tapped @ NGO POI
3
Consent & Biometrics Captured
140
LOCAL (CP Kernel)
Biometric Presence Verified
4
Smartcard and/or Local Data Lake (token Storage)
5
Individual requests access to his/her data
6
Matching Community Pass account found
7
Pod access processed via ID Mgmt Server
8
Access requirements retrieved by Pod Mgmt Server
9
token retrieved from Pod with biometric token data only
10
Re-validate JWT token
11
Reverify biometric presence if token not strong enough
12
2104
PII
Personal Data Store(s) accessed
13
Data read & retrieved
14
Pod data proceses via ID Mgmt Server
15
Community Pass data orchestration service enables Pod Viewer capability
16
EXTERNAL
User Obtains Access to His/Her Data Store at Point of Service (Program Owner)

USE CASE: INDIVIDUAL CAN ACCESS, VIEW, AND UPDATE HIS/HER DATA AT SELECT NETWORK OPERATORS FOR EXAMPLE → A BENEFICIARY CAN VIEW HIS/HER IDENTITY HISTORY AND MAKE CORRECTIONS AS NEEDED

FIG. 21

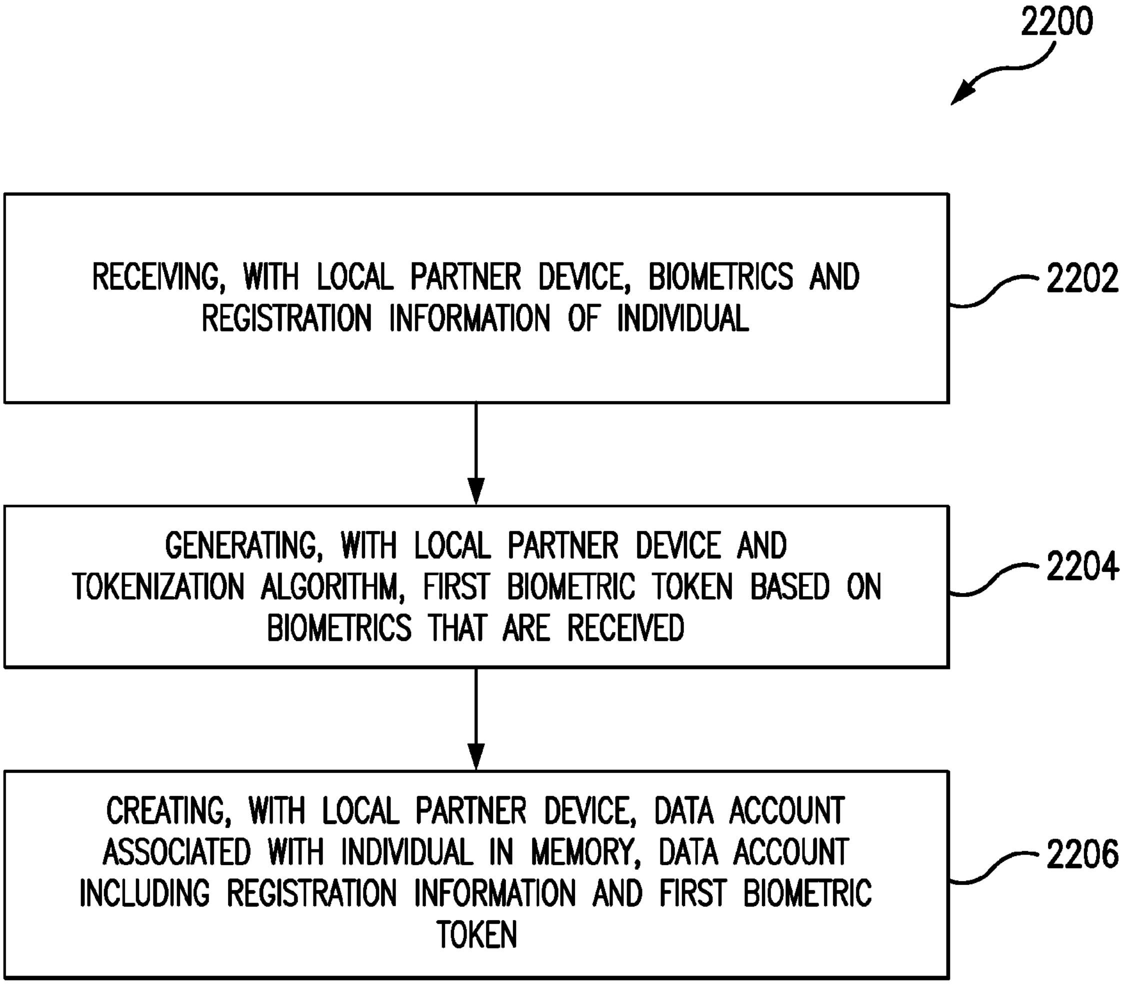

2200
RECEIVING, WITH LOCAL PARTNER DEVICE, BIOMETRICS AND REGISTRATION INFORMATION OF INDIVIDUAL
2202
GENERATING, WITH LOCAL PARTNER DEVICE AND TOKENIZATION ALGORITHM, FIRST BIOMETRIC TOKEN BASED ON BIOMETRICS THAT ARE RECEIVED
2204
CREATING, WITH LOCAL PARTNER DEVICE, DATA ACCOUNT ASSOCIATED WITH INDIVIDUAL IN MEMORY, DATA ACCOUNT INCLUDING REGISTRATION INFORMATION AND FIRST BIOMETRIC TOKEN
2206

FIG. 22

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2021/027706

A. CLASSIFICATION OF SUBJECT MATTER

IPC (20210101) G06F 21/32, H04L 29/06, H04L 9/32, H04W 12/08
CPC (20151101) G06F 21/32, H04L 63/0861, H04L 9/32, H04W 12/08

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC (20210101) G06F 21/32, H04L 29/06, H04L 9/32, H04W 12/08
CPC (20151101) G06F 21/32, H04L 63/0861, H04L 9/32, H04W 12/08

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

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

Databases consulted: Esp@cenet, Google Patents, Orbit, Similari (AI-based)
Search terms used: compare, token+,biometric, tokenization, token

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 3257194 A1 VISA INT SERVICE ASS 20 Dec 2017 (2017/12/20) System 100, biometric input device 110, challenge biometric input device 112, secure server 120, secure database 122, processor 602, memory 604, communication component 638, processor 660, communication component 668, ¶¶25, 38, 81, 119	1-20
A	US 5280527 A KAMAHIRA SAFE CO INC 18 Jan 1994 (1994/01/18) Entire document	1-20
A	US 2016241403 A1 NOK NOK LABS INC 18 Aug 2016 (2016/08/18) Entire document	1-20

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 26 Jul 2021	Date of mailing of the international search report 28 Jul 2021
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Email address: pctoffice@justice.gov.il	Authorized officer BARACH Chev Telephone No. 972-73-3927232

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2021/027706

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
EP 3257194 A1	20 Dec 2017	EP 3257194 A1	20 Dec 2017
		EP 3257194 A4	03 Oct 2018
		EP 3257194 B1	15 Apr 2020
		AU 2016217549 A1	22 Jun 2017
		AU 2016217549 B2	23 Jan 2020
		BR 112017016468 A2	10 Apr 2018
		CN 107251477 A	13 Oct 2017
		CN 107251477 B	12 Jan 2021
		CN 112528258 A	19 Mar 2021
		RU 2017131519 A	12 Mar 2019
		RU 2017131519 A3	09 Sep 2019
		RU 2718226 C2	31 Mar 2020
		US 2017264599 A1	14 Sep 2017
		US 10313317 B2	04 Jun 2019
		US 2019260721 A1	22 Aug 2019
		US 10681025 B2	09 Jun 2020
		WO 2016128906 A1	18 Aug 2016
US 5280527 A	18 Jan 1994	US 5280527 A	18 Jan 1994
		CA 2105404 A1	03 Mar 1995
US 2016241403 A1	18 Aug 2016	US 2016241403 A1	18 Aug 2016
		US 9450760 B2	20 Sep 2016
		CN 106575416 A	19 Apr 2017
		CN 106575416 B	04 Dec 2020
		EP 3175414 A1	07 Jun 2017
		EP 3175414 A4	21 Mar 2018
		EP 3175414 B1	29 Jul 2020
		JP 2017530586 A	12 Oct 2017
		JP 6648110 B2	14 Feb 2020

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2021/027706

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
		KR 20170039672 A	11 Apr 2017
		WO 2016019086 A1	04 Feb 2016