



(51) International Patent Classification:

H04L 29/06 (2006.01) G06F 21/32 (2013.01)
H04L 9/32 (2006.01)

(21) International Application Number:

PCT/US2019/064125

(22) International Filing Date:

03 December 2019 (03.12.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/779,874 14 December 2018 (14.12.2018) US

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

(72) Inventors: **NARAYANSWAMY, Raman**; 3 Sandstone Drive, Nashua, NH 03063 (US). **PRASZCZALEK, Przemek**; 52 Hudson Avenue, Apt 2, Irvington, NY 10533 (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, 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,

(54) Title: SYSTEMS, METHODS, AND NON-TRANSITORY COMPUTER-READABLE MEDIA FOR SECURE INDIVIDUAL IDENTIFICATION

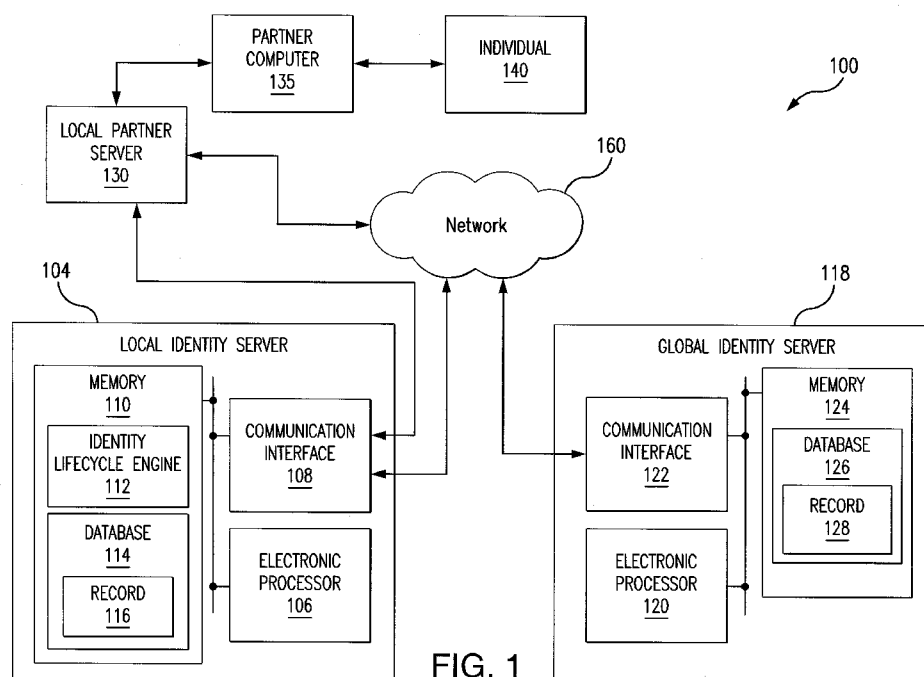


FIG. 1

(57) Abstract: A privacy-enhancing system, method, and non-transitory computer-readable medium for securely identifying an individual over time without retaining sensitive biometric data. In one embodiment, the system includes a local identity server including an electronic processor, a communication interface, and a memory. The electronic processor is configured to initiate a personalization of a partner-specific identification vehicle that identifies the individual based at least in part on an individual global unique identifier associated with the individual, receive a request for a service from the individual via the communication interface, receive consent and registration information from the individual via the communication interface, generate an identity confirmation that confirms an identity of the individual, and output the identity confirmation via the communication interface. The individual global unique identifier is generated from information derived from the registration information and the individual global unique identifier is not indicative of

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

CROSS-REFERENCE TO RELATED APPLICATION

This application claims the benefit of U.S. Provisional Application No.
5 62/779,874, filed on December 14, 2018, the entire content of which is hereby
incorporated by reference.

FIELD OF THE INVENTION

The present disclosure relates generally to secure identification. More
specifically, the present disclosure relates privacy-enhancing systems, methods, and
10 non-transitory computer-readable media.

BACKGROUND

A partner-specific identification vehicle (or other form factor) issued to
an individual by a partner uniquely identifies the individual to that partner. For
example, the partner-specific identification vehicle may contain personally
15 identifiable information (also referred to as "PII") or the partner-specific identification
vehicle may access the PII of the individual on the partner's server. In particular, the
partner-specific identification vehicle may store an individual's biometric data (one
form of PII) or other detailed information that personally identifies the individual.

However, with the increasing number of cyber-attacks on various
20 entities, the risk of exposing the individual's PII is increasing. Once an individual's
PII is obtained by a nefarious actor, the risk of an identity theft or fraud on the
individual is high because the nefarious actor may use the individual's PII to pretend
to be the individual.

SUMMARY

25 The present disclosure relates to privacy-enhancing systems, methods,
and non-transitory computer-readable media that provide for a partner-specific
identification vehicle and identifies an individual without compromising or retaining
any of the individual's PII. By not comprising any of the individual's PII, the
systems, methods, and non-transitory computer-readable media of the present
30 disclosure improve computer security because a nefarious actor cannot commit

identity theft or fraud on the individual even after gaining access to information on the individual's partner-specific identification vehicle.

One embodiment of the present disclosure includes a system for securely identifying an individual. The system includes a local identity server including a first electronic processor, a first communication interface, and a first memory. The first electronic processor is configured to initiate a personalization of a partner-specific identification vehicle that identifies the individual based at least in part on an individual global unique identifier associated with the individual, receive a request for a service from the individual via the first communication interface, receive consent and registration information from the individual via the first communication interface, generate an identity confirmation that confirms an identity of the individual, and output the identity confirmation via the first communication interface, wherein the individual global unique identifier is generated from information derived from the registration information, and wherein the individual global unique identifier is not indicative of personally identifiable information (PII) of the individual.

Another embodiment of the present disclosure includes a method for securely identifying an individual. The method includes initiating, with a local identity server, a personalization of a partner-specific identification vehicle that identifies the individual based at least in part on an individual global unique identifier associated with the individual. The method includes receiving, with the local identity server, a request for a service from the individual via a network. The method includes receiving, with the local identity server, consent and registration information from the individual via the network. The method includes generating, with the local identity server, an identity confirmation that confirms an identity of the individual. The method also includes outputting, with the local identity server, the identity confirmation to the network. In this embodiment, the individual global unique identifier is generated from information derived from the registration information, and the individual global unique identifier is not indicative of personally identifiable information of the individual.

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 initiating a personalization of a partner-specific identification vehicle that identifies an individual based at least in part on an

individual global unique identifier associated with the individual. The set of operations includes receiving a request for a service from the individual via a network. The set of operations includes receiving consent and registration information from the individual via the network. The set of operations includes
5 generating an identity confirmation that confirms an identity of the individual. The set of operations also includes outputting the identity confirmation to the network. In this embodiment, the individual global unique identifier is generated from information derived from the registration information, and the individual global unique identifier is not indicative of personally identifiable information of the individual.

10 BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 illustrates an example system for securely identifying an individual.

FIG. 2 illustrates a secure identity lifecycle with biometrics.

15 FIG. 3 illustrates a registration phase of the secure identity lifecycle with biometrics.

FIG. 4 illustrates an issuance phase of the secure identity lifecycle with biometrics.

FIG. 5 illustrates an identity authentication phase of the secure identity lifecycle with biometrics.

20 FIG. 6 illustrates a first identity management phase of the secure identity lifecycle with biometrics.

FIG. 7 illustrates a second identity management phase of the secure identity lifecycle with biometrics.

FIG. 8 illustrates a secure identity lifecycle without biometrics.

25 FIG. 9 illustrates a registration phase of the secure identity lifecycle without biometrics.

FIG. 10 illustrates an issuance phase of the secure identity lifecycle without biometrics.

FIG. 11 illustrates a token issuance process of the example system of

30 FIG. 1.

FIG. 12 illustrates a successful token matching process of the example system of FIG. 1.

FIG. 13 illustrates an unsuccessful token matching process of the example system of FIG. 1.

FIG. 14 illustrates a second example system for securely identifying an individual.

5 FIG. 15 illustrates one example implementation of the identity network/switch of FIG. 14.

FIG. 16 illustrates another example implementation of the identity network/switch of FIG. 14.

10 FIG. 17 is a flowchart illustrating one example method for securely identifying an individual with the example system of FIG. 1.

DETAILED DESCRIPTION OF THE EMBODIMENTS

The following description is composed of five different sections. The first section (FIG. 1) highlights an example system for securely identifying an individual. The second section (FIGS. 2–7) highlights the issuance of an identity vehicle using biometrics with no PII revealed by identity vehicle or otherwise collected using the example system of FIG. 1. The third section (FIGS. 8–10) highlights where the issuance of an identity vehicle happens in an environment where there are no biometrics or no biometrics yet, so detailed information is collected instead of using the biometrics of the example system of FIG. 1. The fourth section (FIGS. 11–13) highlights a process for token issuance and matching as part of the process that uses biometrics and the example system of FIG. 1. The fifth section (FIGS. 14–16) highlights an identity network/switch in the second example system of FIG. 14. The last section (FIG. 17) highlights a method for securely identifying an individual with the example system of FIG. 1.

25 FIG. 1 illustrates an example system 100 for securely identifying an individual. In the example of FIG. 1, the system 100 includes a local identity server 104, a global identity server 118, a local partner server 130, a partner computer 135, an individual 140, and a network 160.

30 The local identity server 104 and the global identity server 118 may be owned by, or operated by or on behalf of, an administrator. The 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
5 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
10 communication interface 108. For example, all or part of memory 110 may be housed on the “cloud.”

The 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.
15 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
20 a non-transitory computer-readable medium. The memory 124 may be, at least in part, implemented as network storage that is external to the 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.”

The identity lifecycle engine 112 may be stored within a transitory or
25 non-transitory portion of the memory 110. The identity lifecycle engine 112 includes machine readable instructions that are executed by processor 106 to perform the functionality of the local identity server 104 as described below with respect to FIGS. 2–13.

The memory 110 may include a database 114 for storing information
30 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. The database 114 may include a plurality of records. 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 1440, and other N records may be respectively associated with one of N other individuals (not expressly shown in FIG. 1).

The local partner server 130 is in data communication with the partner computer 135. The partner computer 135 may be web-compatible mobile computer, such as an Apple laptop, an Android tablet, a Google smart phone, etc. Alternately, or in addition, the partner computer 135 may be a desktop computer. The partner computer 135 includes an electronic processor in communication with memory. In an embodiment, the electronic processor of the computer 135 is also in communication with a biometric scanner and a communication interface. 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, et cetera) 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 the partner computer 135 to perform the functions of the partner computer 135 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 partner server 130.

The partner computer 135 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 partner computer 135 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 partner computer 135 may communicate with the local partner server 130 over 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 server 130 may include an Application Programming Interface (API) that allows the individual 140 to communicate with the local partner server 130 via the partner computer 135. The local partner server 130 may directly communicate with the local identity server 104 or indirectly communicate over network 160.

The local partner server 130 has an electronic processor in communication with memory. The electronic processor is a microprocessor or another suitable processing device, and the memory is one or more of volatile memory and non-volatile memory (including memory remote from the partner computer 135 and accessible thereby over a network).

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

The local identity server 104 may likewise communicate with partner servers other than the local partner server 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 assistance (e.g., a refugee in a refugee camp, a person who receives aid, etc.). The workings of the local identity server 104 and the local partner server 130 will now be described in additional detail with FIGS. 2–13.

With respect to FIGS. 2–7, the system 100 enrolls the individual 140 using biometrics, issues a partner-specific identification asset, and identifies the individual 140 with the partner-specific identification asset and without exposing or compromising any PII regarding the individual 140. With respect to FIGS. 8–10, the system 100 enrolls the individual 140 using detailed information instead of biometrics, issues a partner-specific identification asset, and identifies the individual 140 with the partner-specific identification asset and without exposing or compromising any PII regarding the individual 140. Lastly, with respect to FIGS. 11–13, the system 100 issues a token, verifies that the individual 140 is the cardholder with an on-card biometric verification, and confirms a relationship between the individual 140 and a partner based at least in part on the token and without exposing or compromising any PII regarding the individual 140.

FIG. 2 illustrates a secure identity lifecycle 200 with biometrics. In the example of FIG. 2, the individual 140 requests enrollment in a program or service

offered by a partner via the local partner server 130. For example, the individual 140 may visit the partner to access the partner computer 135 and enroll.

The local partner server 130 captures the registration of the individual 140 and outputs the registration information to the local identity server 104. The
5 individual 140 also indicates consent to the local partner server 130 and/or the local identity server 104.

As part of registering, the individual 140 provides biometric data associated with the individual 140. For example, the individual undergoes a facial scan, a fingerprint scan, an iris scan, or other suitable biometric scan. The biometric
10 data associated with the individual 140 is included in the registration information that is output by the local partner server 130 to the local identity server 104.

The local identity server 104 captures the biometric data (including images) and generates a biometric template based on the biometric data. After generating the biometric template, the local identity server 104 generates a
15 biometrically-derived hash that includes no biometric data (hereinafter referred to as “biometric hash”) and clears the biometric image, the biometric template, and any biometric data associated with the individual 140 from temporary memory. That is, once the biometric template is generated, the biometric template temporarily persists in the short-term/cache memory until a successful creation of a hash, which triggers a
20 memory flush. For example, the local identity server 104 may use the Trust Stamp™ technology to generate the biometric hash from the biometric template.

Although not shown in FIG. 2, if the biometric hash is unable to be generated from the biometric template, the local identity server 104 either clears the biometric template from temporary memory and attempts to generate another
25 biometric template from the biometric data or clears both the biometric template and the biometric data from the temporary memory and requests additional biometric data from the individual 140.

After successfully generating the biometric hash, the local identity server 104 performs de-duplication using predictive matching to determine whether
30 the biometric hash matches any existing biometric hashes stored in the database 114. For example, the local identity server 104 may use the Trust Stamp™ technology to perform predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the database 114. After checking against existing biometric hashes in the database 114, the local identity server 104 either generates a

new global unique identifier (GUID) associated with the individual 140 and stores the GUID and the biometric hash in the database 114 or simply stores the biometric hash to an existing GUID associated with the individual 140.

After storing the biometric hash, the local identity server 104 generates
5 a token based on the GUID of the individual 140 and the GUID of the partner associated with the local partner server 130. Upon generating the token, the local identity server 104 stores the identification status of the individual 140, the consent of the individual 140, the token associated with the individual 140, and the GUID associated with the individual 140 in the database 114. The local identity server 104
10 also shares some of the identity elements with the partner.

After storing all of the information associated with the individual 140 in the database 114, the local identity server 104 generates a personalization packet (e.g., the biometric hash, the GUID, and/or the token) of the individual 140 and initiates the personalization of an identification asset (e.g., an near field
15 communication (NFC) identification card) as well as the delivery of the identification asset to the partner. The above-described enrollment between the individual 140, the local partner server 130, and the local identity server 104 is an offline enrollment.

FIG. 3 illustrates a registration phase 300 of the secure identity lifecycle 200 with biometrics of FIG. 2. In the example of FIG. 3, the individual 140
20 requests enrollment in a program (e.g., a livelihoods program) or service offered by a partner via the local partner server 130. For example, the individual 140 may visit the partner to access the partner computer 135 and enroll.

The local partner server 130 captures the registration of the individual 140 and outputs the registration information to the local identity server 104. The
25 individual 140 also indicates consent to the local partner server 130 and/or the local identity server 104.

As part of registering, the individual 140 provides biometric data associated with the individual 140. For example, the individual undergoes a facial scan, a fingerprint scan, an iris scan, or other suitable biometric scan. The biometric
30 data associated with the individual 140 is included in the registration information that is output by the local partner server 130 to the local identity server 104.

The local identity server 104 captures the biometric data (including images) and generates a biometric template based on the biometric data. After generating the biometric template, the local identity server 104 generates a biometric

hash and clears the biometric template, the biometric image, and any biometric data associated with the individual 140 from temporary memory. Although not shown in FIG. 2, if the biometric hash is unable to be generated from the biometric template, the local identity server 104 either clears the biometric template from temporary
5 memory and attempts to generate another biometric template from the biometric data or clears both the biometric template and the biometric data from the temporary memory and requests additional biometric data from the individual 140.

After successfully generating the biometric hash, the local identity server 104 performs de-duplication using predictive matching to determine whether
10 the biometric hash matches any existing biometric hash records stored in the database 114. Upon determining that the biometric hash matches an existing record, the local identity server 104 appends the generated biometric hash to the record and outputs a confirmation of a successful biometric capture to the individual 140 via the local partner server 130.

15 Additionally, the identification status of the individual 140, the consent of the individual 140 are stored in the database 114. The local identity server 104 also shares some of the identity elements with the partner.

FIG. 4 illustrates an issuance phase 400 of the secure identity lifecycle 200 with biometrics of FIG. 2. In the example of FIG. 4, after successfully generating
20 the biometric hash, the local identity server 104 performs local de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the database 114. After checking against existing biometric hashes in the database 114, the local identity server 104 either generates a new global unique identifier (GUID) associated with the individual 140 and stores the
25 GUID and the biometric hash in the database 114 or simply stores the biometric hash to an existing GUID associated with the individual 140.

After storing the biometric hash, the local identity server 104 generates a token based on the GUID of the individual 140 and the GUID of the partner associated with the local partner server 130. Upon generating the token, the local
30 identity server 104 stores the identification status of the individual 140, the consent of the individual 140, the token associated with the individual 140, and the GUID associated with the individual 140 in the database 114.

After storing all of the information associated with the individual 140 in the database 114, the local identity server 104 may transmit the biometric hash to

the global identity server 118 via the network 160. In other words, when “online,” the local identity server 104 send biometric hashes to the global identity server 118.

After receiving the biometric hash from the local identity server 104, the global identity server 118 performs global de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the global database 126. After checking against existing biometric hashes in the global database 126, the global identity server 118 stores the biometric hash associated with the individual 140.

After storing all of the information associated with the individual 140 in the database 114, the local identity server 104 generates a personalization packet (e.g., the biometric has, the GUID, and/or the token) of the individual 140 and initiates the personalization of an identification asset (e.g., an near field communication (NFC) identification card) as well as the delivery of the identification asset to the partner.

FIG. 5 illustrates an identity authentication phase of the secure identity lifecycle with biometrics of FIG. 2. In the example of FIG. 5, the individual 140 uses the identification asset and ID profile that was created with the personalization packet described above in FIG. 4 at the partner’s premise. The individual 140 also submits new biometric data using a previous biometric modality. The local partner server 130 passes the information of the individual 140 through to the local identity server 104.

After receiving the ID profile containing a first biometric hash and the new biometric data, the local identity server 104 looks up any records corresponding to the individual 140. The local identity server 104 also generates a biometric template from the new biometric data and generates a second biometric hash from the biometric template. The local identity server 104 authenticates the identity of the individual 140 by performing de-duplication between the first biometric hash and the second biometric hash.

If a match between the first biometric hash and the second biometric hash is at or above a threshold level (e.g., 90% similarity), the hashes are considered to match. If a match between the first biometric hash and the second biometric hash is below a threshold level (e.g., 90% similarity), the hashes are considered to not match. The threshold is not a static level, but rather a dynamic level. For example, the age of the individual 140 may be considered when applying the threshold level to

compensate for any growth that has occurred since the first biometric hash was generated.

After determining there is a match between the first biometric hash and the second biometric hash, the local identity server 104 authenticates the session with the individual 140. The local server 104 also stores the successful authentication in the record 116 associated with the individual 140 and outputs the successful authentication to the local partner server 130. The local partner server 130 may store the successful authentication in its own database.

FIG. 6 illustrates a first identity management phase 600 of the secure identity lifecycle with biometrics of FIG. 2. In the example of FIG. 6, the individual 140 uses the identification asset and ID profile that was created with the personalization packet described above in FIG. 4 at the partner. The individual 140 submits new biometric data using a new biometric modality (e.g., an iris scan) as well as providing new consent to the new biometric data.

The local identity server 104 generates a biometric template from the new biometric data and generates a second biometric hash (e.g., an iris-based hash) from the biometric template. Additionally, after receiving the ID profile containing a first biometric hash (e.g., a fingerprints-based hash) and the new biometric data, the local identity server 104 looks up any records corresponding to the individual 140. For example, the local identity server 104 looks up whether the individual 140 has any existing biometric hashes. Upon determining there are existing biometric hashes, the local identity server 104 determines the types of the existing biometric hashes. The local identity server 104 maintains the identity of the individual 140 by performing de-duplication between the first biometric hash and the second biometric hash to detect the new biometric hash modality.

FIG. 7 illustrates a second identity management phase 700 of the secure identity lifecycle with biometrics of FIG. 2. In the example of FIG. 7, the local identity server 104 receives information regarding the use of the identification asset and ID profile that was created with the personalization packet described above in FIG. 4 at the partner. The local identity server 104 also receives new biometric data using a new biometric modality (e.g., an iris scan).

The local identity server 104 generates a biometric template from the new biometric data and generates a second biometric hash (e.g., an iris-based hash) from the biometric template. Additionally, after receiving the ID profile containing a

first biometric hash (e.g., a fingerprints-based hash) and the new biometric data, the local identity server 104 looks up any records corresponding to the individual 140. For example, the local identity server 104 looks up whether the individual 140 has any existing biometric hashes (e.g., biometric hashes associated with other partners).

5 Upon determining there are existing biometric hashes, the local identity server 104 determines the types of the existing biometric hashes. The local identity server 104 maintains the identity of the individual 140 by performing de-duplication between the first biometric hash and the second biometric hash to detect the new biometric hash modality. After detecting there is a new biometric hash modality, the local identity

10 server 104 stores the second biometric hash in the record 116 associated with the individual 140 and updates the identification asset to include the second biometric hash.

FIG. 8 illustrates a secure identity lifecycle 800 without biometrics. In the example of FIG. 8, the individual 140 requests enrollment in a program or service

15 offered by a partner via the local partner server 130. For example, the individual 140 may visit the partner to access the partner computer 135 and enroll.

The local partner server 130 captures the registration of the individual 140 and outputs the registration information to the local identity server 104. The individual 140 also indicates consent to the local partner server 130 and/or the local

20 identity server 104.

As part of registering, the individual 140 provides detailed information associated with the individual 140. The detailed information associated with the individual 140 is included in the registration information that is output by the local partner server 130 to the local identity server 104.

25 The local identity server 104 performs de-duplication on data fields and generates an individual global unique identifier (GUID) associated with the individual 140. The local identity server 104 also generates a unique identifier (e.g., a web ID including the public individual GUID) that is public. After generating the unique identifier, the local identity server 104 generates a personal identification

30 number (PIN) and username and establishes a user data store associated with the individual 140 in the database 114.

After establishing the user data store, the local identity server 104 generates a token based on the GUID of the individual 140 and the GUID of the partner associated with the local partner server 130. Upon generating the token, the

local identity server 104 stores the unique identifier of the individual 140, the identification status of the individual 140, the consent of the individual 140, the token associated with the individual 140, and the GUID associated with the individual 140 in the database 114. The local identity server 104 also shares some of the identity elements with the local partner server 130.

After storing all of the information associated with the individual 140 in the database 114, the local identity server 104 generates a personalization packet (e.g., the biometric hash, the GUID, and/or the token) of the individual 140 and initiates the personalization of an identification asset (e.g., an near field communication (NFC) identification card) as well as the delivery of the identification asset to the partner. The above-described enrollment between the individual 140, the local partner server 130, and the local identity server 104 is an offline enrollment.

FIG. 9 illustrates a registration phase 900 of the secure identity lifecycle 800 without biometrics. In the example of FIG. 9, the individual 140 requests enrollment in a program or service offered by a partner via the local partner server 130. For example, the individual 140 may visit the partner to access the partner computer 135 and enroll.

The local partner server 130 captures the registration of the individual 140 and outputs the registration information to the local identity server 104. The individual 140 also indicates consent to the local partner server 130 and/or the local identity server 104.

As part of registering, the individual 140 provides detailed information associated with the individual 140. The detailed information associated with the individual 140 is included in the registration information that is output by the local partner server 130 to the local identity server 104.

The local identity server 104 performs de-duplication on data fields to determine whether the individual is already enrolled. Upon determining that the individual is not enrolled, the local identity server 104 generates a user global unique identifier (GUID) associated with the individual 140. The local identity server 104 also generates a unique identity profile (e.g., a web ID) that is public. After generating the unique identity profile, the local identity server 104 confirms the successful creation of the ID profile. Upon determining that the individual is enrolled, the local identity server 104 updates or appends data elements in an existing

ID profile that is associated with the individual 140. After updating the ID profile, the local identity server 104 confirms the successful update of the ID profile.

FIG. 10 illustrates an issuance phase 1000 of the secure identity lifecycle 800 without biometrics. In the example of FIG. 10, the local identity server 104 performs de-duplication on data fields and generates two user global unique identifier (GUID) associated with the individual 140. One of the two individual GUIDs is public and the other of the two individual GUIDs is private.

The local identity server 104 also generates a unique identifier (e.g., a Web ID, including the public individual GUID) that is public. After generating the unique identifier, the local identity server 104 generates a personal identification number (PIN) and username and establishes a user data store associated with the individual 140 in the database 114.

After establishing the user data store, the local identity server 104 generates a token based on the private GUID of the individual 140 and the GUID of the partner associated with the local partner server 130. Upon generating the token, the local identity server 104 stores the unique identifier of the individual 140, the identification status of the individual 140, the consent of the individual 140, the token associated with the individual 140, and the private GUID associated with the individual 140 in the database 114. The local identity server 104 also shares some of the identity elements with the local partner server 130.

After storing all of the information associated with the individual 140 in the database 114, the local identity server 104 generates a personalization packet (e.g., the unique identifier, the GUID, and/or the token) of the individual 140 and initiates the personalization of an identification asset (e.g., an near field communication (NFC) identification card) as well as the delivery of the identification asset to the partner.

FIG. 11 illustrates a token issuance process 1100 of the example system of FIG. 1. In the example of FIG. 11, the local identity server 104 performs local de-duplication of information from the individual 140 and generates a global unique identifier (GUID) or “G” that is private (i.e., based on detailed information provided by the individual 140) or biometrically derived (i.e., based on biometric data provided by the individual 140).

The local identity server 104 generates a token “T” by combining the GUID “G” with the partner global unique identifier “P” that is private. The local

identity server 104 stores the identification status, the token “T”, the GUID “G”, and the partner GUID “P” in the database 114. The local identity server 104 may also share some of the ID data elements with the local partner server 130 (e.g., the partner GUID “P” and the token “T”).

5 After storing all of the information associated with the individual 140 in the database 114, the local identity server 104 generates a personalization packet (e.g., the GUID and/or the token) of the individual 140 and initiates the personalization of an identification asset (e.g., an near field communication (NFC) identification card) as well as the delivery of the identification asset to the partner
10 and/or the individual.

FIG. 12 illustrates a successful token matching process 1200 of the example system of FIG. 1. In the example of FIG. 12, the individual 140 brings the identification asset (e.g., the NFC smartcard) to the partner and the partner computer. The local identity server 104 confirms an authentication of the biometric hash on the
15 card based an on-card biometric match (e.g., the authentication phase 500 of FIG. 5).

After confirming an on-card biometric match, the local identity server 104 retrieves the ID profile and the biometric hash stored on the identification asset via the local partner server 130 and the partner computer 135. Specifically, the local identity server 104 retrieves the individual GUID stored on the identification asset.

20 Additionally, after confirming the on-card biometric match, the local identity server 104 retrieves the token associated with the individual 140 and the partner GUID from the local partner server 130. The local identity server 104 uses the individual GUID “G” and the partner GUID “P” to generate a new context token. The local identity server 104 then uses a matching technique to compare the new
25 content token to the token retrieved from the local partner server 130.

Upon determining the new context token matches the token retrieved from the local partner server 130, the local identity server 104 captures the successful relationship match and captures the identification asset interaction. The local identity server 104 also authenticates the session and outputs confirmation of the authenticated
30 session to the local partner sever 130. Upon receiving confirmation, the local partner server 130 clears the individual 140 to proceed.

FIG. 13 illustrates an unsuccessful token matching process 1300 of the example system of FIG. 1. In the example of FIG. 13, the individual 140 brings the identification asset (e.g., the NFC smartcard) to the partner and the partner computer.

The local identity server 104 confirms an authentication of the biometric hash on the card based on an on-card biometric match (e.g., the authentication phase 500 of FIG. 5).

After confirming an on-card biometric match, the local identity server 104 retrieves the ID profile and the biometric hash stored on the identification asset via the local partner server 130 and the partner computer 135. Specifically, the local identity server 104 retrieves the individual GUID stored on the identification asset.

Additionally, after confirming the on-card biometric match, the local identity server 104 retrieves the token associated with the individual 140 and the partner GUID from the local partner server 130. The local identity server 104 uses the individual GUID “G” and the partner GUID “P” to generate a new context token. The local identity server 104 then uses predictive matching to compare the new content token to the token retrieved from the local partner server 130.

Upon determining the new context token does not match the token retrieved from the local partner server 130, the local identity server 104 captures the unsuccessful relationship match and the unauthorized relationship attempt (whether friendly or unfriendly). The local identity server 104 also rejects the session and outputs an indication that the user-partner unique relation is not confirmed to the local partner server 130. Upon receiving the indication, the local partner server 130 does not clear the individual 140 to proceed. A number of possible exceptions processing actions may be designed and initiated at that stage to guide a response to this event. For example, the exceptions processing actions may include one or more of rejecting the authentication attempt, creating a record of a potential fraud attempt, sending the unmatched token to the global data store for “matching” and flagging profile of individual associated with the unmatched token, performing an alternate method of authentication, or other suitable exceptions processing action.

As illustrated in FIG. 13, in some examples, the local identity server 104 searches the database 114 to find a token that matches the new context token. Upon determining a match between a token in the database 114 and the new context token, the local identity server 104 determines an individual that is linked to the new context token and flags that relationship for possible review.

Thus, as has been described, the system 100 may, among other things, allow the individual 140 to be securely identified without compromising the PII of the individual 140.

FIG. 14 illustrates a second example system 1400 for securely identifying an individual. In the example of FIG. 14, the system 1400 includes an identity (ID) network/switch 1402 as part of a local identity server 1404, a plurality of local partner servers 1406A–1406N, legacy servers 1408, a global identity server 1418, and an individual 1440.

In the example of FIG. 14, the identity (ID) network/switch 1402 interconnects the biometric services of the local identity server 1404, the legacy servers 1408, and the global identity server 1418. In some examples, the local identity server 1404 is the same or similar to the local identity server 104; each local partner server of the plurality of local partner servers 1406A–1406N is the same or similar to the local partner server 130; and the global identity server 1418 is the same or similar to the global identity server 118, respectively, as described above in FIGS. 1–13. Consequently, the redundant description of the local identity server 1404, the plurality of local partner servers 1406A–1406N, and the global identity server 1418 is not repeated herein.

As illustrated in FIG. 14, each of the plurality of local partner servers 1406A–1406N includes an agency application with an identity software development kit (ID SDK). The ID SDK is a program that differentiates between standardized biometric templates associated with the local identity server 1404 and/or the global identity server 1418, and proprietary biometric templates associated with one or more of the legacy servers 1408. For example, when the individual 1440 requests a service from the local partner server 1406A and provides a standardized biometric template from an individual resource (e.g., an identification vehicle), the local partner server 1406A routes the standardized biometric template to the global identity server 1418 via the local identity server 1404.

However, when the individual 1440 requests a service from the local partner server 1406A and provides a proprietary biometric template from the individual resource, the local partner server 1406A routes the proprietary biometric template to one or more of the legacy servers 1408 via the local identity server 1404. Additionally, in some examples, when the individual 1440 requests a service from the local partner server 1406A and provides a proprietary biometric template from the individual resource, the local partner server 1406A may also route the proprietary biometric template to one or more of the legacy servers 1408 and the global identity server 1418 via the local identity server 1404. In other words, the identity

network/switch 1402 is a network that interconnects various databases to receive identity information from the individual 1440 and one or more databases are targeted based on the type of identity information that is received from the individual 1440.

In the example of FIG. 14, the identity information from the individual
5 1440 may be provided to the global identity server 1418, one or more of the legacy servers 1408, or both without exposing any personally identifiable information (PII). Consequently, the ID network/switch 1402 allows the legacy servers 1408 to interoperate with the local identity server 1404, the global identity server 1418, and the plurality of local partner servers 1406A–1406N without needing to expose any PII
10 that may exist in the legacy servers 1408. In some examples, the legacy servers 1408 may include existing government databases (e.g., a national identity database), financial databases, telecommunication databases, or other suitable legacy databases that include personally identifiable information (PII).

Additionally, as illustrated in FIG. 14, the global identity server 1418
15 includes a biometric hash translation service. However, in other examples, the local identity server 1404 may include the biometric hash translation service. The biometric hash translation service translates the propriety biometric template from either the individual 1440 via the ID network/switch 1402 or the legacy servers 1408 to a biometric hash. The biometric hash may then be stored in the database 126 of the
20 global identity server 1418. Similarly, the biometric hash may also be stored in the database 114 of the local identity server 1404. In other words, the biometric hash translation service in combination with the ID network/switch 1402 increases the number of biometric hashes that are associated with the individual 1440 by converting the proprietary biometric templates that are sent to and associated with the legacy
25 servers 1408 to biometric hashes. The biometric hashes that are converted from the proprietary biometric templates may then be stored locally and/or globally.

FIG. 15 illustrates one example implementation of the identity network/switch 1402 of FIG. 14. In the example of FIG. 15, the individual 1440 requests enrollment in a program or service offered by a partner via the local partner
30 server 1406A. For example, the individual 1440 may visit the partner to access the partner computer 135A and enroll.

The local partner server 1406A captures the registration of the individual 1440 from the partner computer 135A and outputs the registration

information to the local identity server 1404A. The individual 1440 also indicates consent to the local partner server 1406A and/or the local identity server 1404A.

As part of registering, the individual 1440 provides biometric data associated with the individual 1440. For example, the individual undergoes a facial scan, a fingerprint scan, an iris scan, or other suitable biometric scan. The biometric data associated with the individual 1440 is transformed by the local partner server 1406A into a standardized biometric template, which is then associated with the local partner server 1406A. The standardized biometric template and the registration information is output by the local partner server 1406A to the local identity server 1404A.

The local identity server 1404A captures the standardized biometric template and the registration information. The local identity server 1404A generates a biometric hash based on the standardized biometric template and clears both the standardized biometric template and any biometric data associated with the individual 1440 from temporary memory. For example, the local identity server 1404A may use the Trust Stamp™ technology to generate the biometric hash from the standardized biometric template created by the local partner server 1406A.

Although not shown in FIG. 15, if the biometric hash is unable to be generated from the standardized biometric template, the local identity server 1404A clears the standardized biometric template from temporary memory and requests another standardized biometric template from the individual 1440 via the local partner server 1406A.

After successfully generating the biometric hash, the local identity server 1404A performs de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the database 114. For example, the local identity server 1404A may use the Trust Stamp™ technology to perform predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the database 114. After checking against existing biometric hashes in the database 114, the local identity server 1404A either generates a new global unique identifier (GUID) associated with the individual 1440 and stores the GUID and the biometric hash in the database 114 or simply stores the biometric hash to an existing GUID associated with the individual 1440.

After storing all of the information associated with the individual 1440 in the database 114, the local identity server 1404A may transmit the biometric hash to the global identity server 1418 via the network 160. In other words, when “online,” the local identity server 1404A sends biometric hashes to the global identity server
5 1418.

After receiving the biometric hash from the local identity server 1404A, the global identity server 1418 performs global de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the global database 126. After checking against existing
10 biometric hashes in the global database 126, the global identity server 1418 stores the biometric hash associated with the individual 1440.

Additionally, in the example of FIG. 15, the individual 1440 requests enrollment in a program or service offered by a second partner via the local partner server 1406B. For example, the individual 1440 may visit the second partner to
15 access the partner computer 135B and enroll.

The local partner server 1406B captures the registration of the individual 1440 and outputs the registration information to the local identity server 1404B. The individual 1440 also indicates consent to the local partner server 1406B and/or the local identity server 1404B.

20 As part of registering, the individual 1440 provides biometric data associated with the individual 1440. For example, the individual 1440 undergoes a facial scan, a fingerprint scan, an iris scan, or other suitable biometric scan. Additionally, in some examples, the individual 1440 may provide an existing standardized biometric template to the local partner server 1406B. The biometric data
25 associated with the individual 1440 is transformed into a standardized biometric template that is associated with the local partner server 1406B. The standardized biometric template, the registration information, and the existing standardized biometric template are output by the local partner server 1406B to the local identity server 1404B.

30 The local identity server 1404B captures the standardized biometric template, the registration information, and the existing standardized biometric template. The local identity server 1404B performs a hash translation between the standardized biometric template and the existing standardized biometric template and generates a biometric hash based on the hash translation and clears the standardized

biometric template, the existing standardized biometric template, and any biometric data associated with the individual 1440 from the temporary memory. For example, the local identity server 1404B may use the Trust Stamp™ technology to generate the biometric hash from the standardized biometric template created by the local partner server 1406B and the existing standardized template created by the local partner server 1406A.

Although not shown in FIG. 15, if the biometric hash is unable to be generated from the hash translation, the local identity server 1404B may clear the standardized biometric template from temporary memory and request another standardized biometric template from the individual 1440 via the local partner server 1406B.

After successfully generating the biometric hash, the local identity server 1404B performs a record query (i.e., a 1:1 record query for 1:n predictive match) of the individual because the biometric hash is based at least in part on an existing standardized biometric template. The global identity server 1418 outputs any similar biometric hashes to the local identity server 1404B.

The local identity server 1404B performs de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the database 114 and the biometric hashes received from the global identity server 1418. For example, the local identity server 1404B may use the Trust Stamp™ technology to perform predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the database 114 and the biometric hashes received from the global identity server 1418.

In one example, after checking against existing biometric hashes in the database 114 and the biometric hashes received from the global identity server 1418, the local identity server 1404B finds no match and generates a new global unique identifier (GUID) associated with the individual 1440 and stores the GUID and the biometric hash in the database 114. In another example, after checking against existing biometric hashes in the database 114 and the biometric hashes received from the global identity server 1418, the local identity server 1404B finds a match and stores the biometric hash, the existing hashes, and an existing GUID associated with the individual 1440 in the database 114.

After storing all of the information associated with the individual 1440 in the database 114, the local identity server 1404B may transmit the biometric hash

to the global identity server 1418 via the network 160. In other words, when “online,” the local identity server 1404B sends “matched” biometric hashes to the global identity server 1418.

After receiving the biometric hash from the local identity server 1404B, the global identity server 1418 may simply store the biometric hash associated with the individual 1440. In other examples, after receiving the biometric hash from the local identity server 1404B, the global identity server 1418 may perform a global de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the global database 126. After performing the global de-duplication, the global identity server 1418 stores the biometric hash associated with the individual 1440.

In the example of FIG. 15, the identity network/switch 1402 of FIG. 14 is the interconnection between the local partner servers 1406A and 1406B, the local identity servers 1404A and 1404B, and the global identity server 1418. With the above-noted interconnection, the local identity servers 1404A and 1404B continuously update their respective database 114 when the individual 1440 requests a service. Likewise, the global identity server 1418 continuously updates the database 126 when the individual 1440 requests a service. These continuous updates of biometric hashes ensure that the local identity servers 1404A and 1404B and the global identity server 1418 may accurately identify the individual 1440 even as the biometric data of the individual 1440 changes over time. For example, these continuous updates may account for the aging of the individual 1440 over time.

FIG. 16 illustrates another example implementation of the identity network/switch 1402 of FIG. 14. In the example of FIG. 16, the individual 1440 has previously enrolled in a program or service offered by a partner via the local partner server 1406A. For example, the individual 1440 has previously visited the partner to access the partner computer 135A and enroll in a service.

The local partner server 1406A captured the registration of the individual 1440 and output the registration information to the local legacy server 1602 (e.g., one of the legacy servers 1408 as described above in FIG. 14). The individual 1440 also indicated consent to the local partner server 1406A and/or the local legacy server 1602.

As part of registering, the individual 1440 provided biometric data associated with the individual 1440. For example, the individual 1440 underwent a

facial scan, a fingerprint scan, an iris scan, or other suitable biometric scan. The biometric data associated with the individual 1440 is transformed into a proprietary biometric template at the local partner server 1406A based on the proprietary form issued by the local legacy server 1602. The proprietary biometric template, the
5 biometric data, and the registration information is output by the local partner server 1406A to the local legacy server 1602.

The local legacy server 1602 captured the proprietary biometric template, the biometric data, and the registration information. The local legacy server 1602 performed de-duplication using predictive matching of personally identifiable
10 information (PII) to determine whether the proprietary biometric template matches any existing proprietary biometric templates stored in the local legacy server 1602. After checking against existing proprietary biometric templates in the database of the local legacy server 1602, the local legacy server 1602 outputs the proprietary biometric template to the global legacy server 1604.

15 In the example of FIG. 15, after storing the proprietary biometric template, the global legacy server 1604 outputs the proprietary biometric template to the local identity server 1404. The local identity server 1404 uses a hash translation service (as described above in FIG. 14) to translate the proprietary biometric template into a biometric hash. In some examples, the local identity server 1404 transmits the
20 biometric hash to the global identity server 1418, and the global identity server 1418 stores the biometric hash in the database 126.

However, in some examples, to translate the proprietary biometric template into a biometric hash, the local identity server 1404 adjusts the proprietary biometric template into a standards-based and “hash-friendly” template that allows for
25 transformation into a biometric hash. In other words, the proprietary aspect of the proprietary biometric template may need to be removed by the local identity server 1404 to create a “hash-friendly” biometric template that may be hashed by the local identity server 1404. Although the hash translation service is described with respect to the local identity server 1404, the hash translation service may be implemented by
30 any of the servers that store or use the proprietary biometric template.

Additionally, in the example of FIG. 15, the individual 1440 requests enrollment in a program or service offered by a second partner via the local partner server 1406B. For example, the individual 1440 may visit the second partner to access the partner computer 135B and enroll.

The local partner server 1406B captures the registration of the individual 1440 and outputs the registration information to the local identity server 1404. The individual 1440 also indicates consent to the local partner server 1406B and/or the local identity server 1404.

5 As part of registering, the individual 1440 provides biometric data associated with the individual 1440. For example, the individual 1440 undergoes a facial scan, a fingerprint scan, an iris scan, or other suitable biometric scan. Additionally, in some examples, the individual 1440 may provide an existing proprietary biometric template to the local partner server 1406B via a pre-existing
10 individual resource (e.g., an identity card). The biometric data associated with the individual 1440 is transformed into a standardized biometric template. The standardized biometric template, the registration information, and the existing proprietary biometric template are output by the local partner server 1406B to the local identity server 1404. The local identity server 1404 captures the standardized
15 biometric template, the registration information, and the existing proprietary biometric template. The local identity server 1404 generates a biometric hash based on the standardized biometric template and clears the standardized biometric template and any biometric data associated with the individual 1440 from temporary memory. For example, the local identity server 1404 may use the Trust Stamp™ technology to
20 generate the biometric hash from the standardized biometric template created by the local partner server 1406B.

After successfully generating the biometric hash and in response to receiving the existing proprietary biometric template, the local identity server 1404 performs a record query (i.e., a 1:1 record query for 1:n predictive match) regarding
25 the individual 1440. The global identity server 1418 outputs any similar biometric hashes to the local identity server 1404. Additionally, in some examples, the local identity server 1404 may use the hash translation service to translate the existing proprietary biometric template into a biometric hash as described above.

The local identity server 1404 performs de-duplication using predictive
30 matching to determine whether the biometric hash (or biometric hashes) matches any existing biometric hashes stored in the database 114 and the biometric hashes received from the global identity server 1418. For example, the local identity server 1404 may use the Trust Stamp™ technology to perform predictive matching to determine whether the biometric hash (or biometric hashes) matches any existing biometric

hashes stored in the database 114 and the biometric hashes received from the global identity server 1418.

In one example, after checking against existing biometric hashes in the database 114 and the biometric hashes received from the global identity server 1418, the local identity server 1404 finds no match and generates a new global unique identifier (GUID) associated with the individual 1440 and stores the GUID and the biometric hash in the database 114. In another example, after checking against existing biometric hashes in the database 114 and the biometric hashes received from the global identity server 1418, the local identity server 1404 finds a match and stores the biometric hash, the existing hashes match, and the existing GUID associated with the individual 1440 in the database 114.

After storing all of the information associated with the individual 1440 in the database 114, the local identity server 1404 may transmit the biometric hash to the global identity server 1418 via the network 160. In other words, when “online,” the local identity server 1404 sends “matched” biometric hashes to the global identity server 1418.

After receiving the biometric hash from the local identity server 1404, the global identity server 1418 may simply store the biometric hash associated with the individual 1440. In other examples, after receiving the biometric hash from the local identity server 1404, the global identity server 1418 may perform a global de-duplication using predictive matching to determine whether the biometric hash matches any existing biometric hashes stored in the global database 126. After performing the global de-duplication and finding a match, the global identity server 1418 stores the biometric hash associated with the individual 1440.

In the example of FIG. 16, the identity network/switch 1402 of FIG. 14 is the interconnection between the local partner servers 1406A and 1406B, the local identity server 1404, the local legacy server 1602, the global legacy server 1604, and the global identity server 1418. With the above-noted interconnection, the local identity server 1404 continuously updates the database 114 when the individual 1440 requests a service from the first partner or the second partner. Additionally, in some examples, the global identity server 1418 also continuously updates the database 126 when the individual 1440 requests a service from the first partner or the second partner. By continually updating the database 126 and the database 114, the local identity server 1404 and the global identity server 1418 may continue to accurately

identify the individual 1440 even as the biometric data of the individual 1440 changes over time. For example, the local identity server 1404 and the global identity server 1418 may accurately identify the individual 1440 even as the individual 1440 ages over time.

5 FIG. 17 is a flowchart illustrating one example method 1700 for securely identifying an individual with the local identity server 104 in the example system 100 of FIG. 1. FIG. 17 is described with respect to FIG. 1.

 The method 1700 includes initiating, with the local identity server 104, a personalization of a partner-specific identification vehicle that identifies the
10 individual 140 based at least in part on an individual global unique identifier associated with the individual 140 (at block 1702). The method 1700 includes receiving, with the local identity server 104, a request for a service from the individual 140 via the network 160 (at block 1704). The method 1700 includes receiving, with the local identity server 104, consent and registration information
15 from the individual 140 via the network 160 (at block 1706). The method 1700 includes generating, with the local identity server 104, an identity confirmation that confirms an identity of the individual 140 (at block 1708). The method 1700 also includes outputting, with the local identity server 104, the identity confirmation to the network 160 (at block 1710). In this example of the method 1700, the individual
20 global unique identifier is generated from information derived from the registration information, and the individual global unique identifier is not indicative of personally identifiable information of the individual.

 Many different arrangements of the various components depicted, as well as components not shown, are possible without departing from the spirit and
25 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
30 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:

- 5 1. A system for securely identifying an individual, the system comprising:
- a local identity server including a first electronic processor, a first communication interface, and a first memory,
- the first electronic processor is configured to initiate a personalization of a
- 10 partner-specific identification vehicle that identifies the individual based at least in part on an individual global unique identifier associated with the individual,
- receive a request for a service from the individual via the first communication interface,
- receive consent and registration information from the individual via the first
- 15 communication interface,
- generate an identity confirmation that confirms an identity of the individual, and
- output the identity confirmation via the first communication interface,
- wherein the individual global unique identifier is generated from information
- 20 derived from the registration information, and
- wherein the individual global unique identifier is not indicative of personally identifiable information of the individual.
2. The system of claim 1, further comprising:
- 25 a local partner server including a second electronic processor, a second communication interface, and a second memory that are communicatively connected to each other, the second electronic processor is configured to
- receive the request for the service from the individual,
- output the consent and the registration information from the individual via the
- 30 second communication interface,
- receive the identity confirmation via the second communication interface, and
- approve the request for the service from the individual based on the identity confirmation,

wherein the first communication interface and the second communication interface communicate with each other over a network.

3. The system of claim 2, further comprising:
- 5 one or more legacy servers, each of the one or more legacy servers including a third electronic processor, a third communication interface, and a legacy database that are communicatively connected to each other,
- wherein the second electronic processor is further configured to receive a first biometric template of the individual from the partner-specific
- 10 identification vehicle that is assigned to the individual,
- generate a second biometric template of the individual based on the registration information,
- output the first biometric template of the individual and the second biometric template of the individual via the second communication interface,
- 15 wherein the first electronic processor is further configured to receive the first biometric template and the second biometric template via the first communication interface,
- determine whether the first biometric template is associated with one of the one or more legacy servers, and
- 20 output the first biometric template to the one of the one or more legacy servers via the first communication interface in response to determining that the first biometric template is associated with the one of the one or more legacy servers, and
- wherein the first communication interface, the second communication interface, the third communication interface communicate with each other over the
- 25 network.

4. The system of claim 3, further comprising:
- a global identity server including a fourth electronic processor, a fourth communication interface, and a fourth memory that are communicatively connected
- 30 to each other,
- wherein the first electronic processor is further configured to output the first biometric template via the first communication interface, and
- wherein the fourth electronic processor is configured to receive the first biometric template via the fourth communication interface,

translate the first biometric template into a biometric hash,
perform de-duplication to determine whether the biometric hash matches any
other biometric hashes,
associate the biometric hash with the individual global unique identifier that is
5 assigned to the individual in response to determining that the biometric hash matches
a different biometric hash that is already associated with the individual,
store the biometric hash in the fourth memory in response to associating the
biometric hash with the individual global unique identifier, and
output the identity confirmation via the fourth communication interface in
10 response to associating the biometric hash with the individual global unique identifier.

5. The system of claim 3, wherein the first electronic processor is
configured to

translate the first biometric template into a biometric hash,
15 perform de-duplication to determine whether the biometric hash matches any
other biometric hashes,
associate the biometric hash with the individual global unique identifier that is
assigned to the individual in response to determining that the biometric hash matches
a different biometric hash that is already associated with the individual,
20 store the biometric hash in the first memory in response to associating the
biometric hash with the individual global unique identifier, and
output the identity confirmation via the first communication interface in
response to associating the biometric hash with the individual global unique identifier.

25 6. The system of claim 2, further comprising:
a global identity server including a third electronic processor, a third
communication interface, and a third memory that are communicatively connected to
each other,
wherein the second electronic processor is further configured to
30 receive a first biometric template of the individual from the partner-specific
identification vehicle that is assigned to the individual,
generate a second biometric template of the individual based on the
registration information,

output the first biometric template of the individual and the second biometric template of the individual via the second communication interface,
wherein the first electronic processor is further configured to
generate a biometric hash based on the second biometric template, and
5 output the first biometric template and the biometric hash via the first communication interface, and
wherein the third electronic processor is configured to
receive the first biometric template and the biometric hash via the third communication interface,
10 translate the first biometric template into a second biometric hash,
perform de-duplication to determine whether the biometric hash and the second biometric hash match any other biometric hashes,
associate the biometric hash and the second biometric hash with the individual global unique identifier that is assigned to the individual in response to determining
15 that the biometric hash and the second biometric hash match a different biometric hash that is already associated with the individual,
store the biometric hash and the second biometric hash in the third memory in response to associating the biometric hash and the second biometric hash with the individual global unique identifier, and
20 output the identity confirmation via the third communication interface in response to associating the biometric hash and the second biometric hash with the individual.

7. The system of claim 2, wherein the second electronic
25 processor is further configured to
receive a first biometric template of the individual from the partner-specific identification vehicle that is assigned to the individual,
generate a second biometric template of the individual based on the registration information,
30 output the first biometric template of the individual and the second biometric template of the individual via the second communication interface, and
wherein the first electronic processor is configured to
generate a biometric hash based on the second biometric template,
translate the first biometric template into a second biometric hash,

perform de-duplication to determine whether the biometric hash and the second biometric hash match any other biometric hashes,

associate the biometric hash and the second biometric hash with the individual global unique identifier that is assigned to the individual in response to determining
5 that the biometric hash and the second biometric hash match a different biometric hash that is already associated with the individual,

store the biometric hash and the second biometric hash in the second memory in response to associating the biometric hash and the second biometric hash with the individual global unique identifier, and

10 output the identity confirmation to the local partner server via the second communication interface in response to associating the biometric hash and the second biometric hash with the individual global unique identifier.

8. The system of claim 2, wherein the second electronic processor
15 is further configured to

generate a biometric template of the individual based on the registration information, and

output the biometric template of the individual via the second communication interface.

20 9. The system of claim 8, wherein the first electronic processor is configured to

receive the biometric template via the first communication interface,

generate a biometric hash based on the biometric template,

25 perform de-duplication to determine whether the biometric hash matches any other biometric hashes,

associate the biometric hash with the individual global unique identifier that is assigned to the individual in response to determining that the biometric hash matches a different biometric hash that is already associated with the individual,

30 store the biometric hash in the second memory in response to associating the biometric hash with the individual global unique identifier, and

output the identity confirmation via the first communication interface in response to associating the biometric hash with the individual global unique identifier.

10. The system of claim 8, further comprising:
a global identity server including a third electronic processor, a third communication interface, and a third memory that are communicatively connected to each other,
- 5 wherein the first electronic processor is further configured to receive the biometric template via the first communication interface, generate a biometric hash based on the biometric template, and output the biometric hash via the first communication interface, wherein the third electronic processor is configured to
- 10 receive the biometric hash via the third communication interface, perform de-duplication to determine whether the biometric hash matches any other biometric hashes,
- associate the biometric hash with the individual global unique identifier that is assigned to the individual in response to determining that the biometric hash matches
- 15 a different biometric hash that is already associated with the individual,
- store the biometric hash in the third memory in response to associating the biometric hash with the individual global unique identifier, and
- output the identity confirmation to the local partner server via the third communication interface in response to associating the biometric hash with the
- 20 individual global unique identifier, and
- wherein the first communication interface, the second communication interface, the third communication interface communicate with each other over the network.

- 25 11. A method for securely identifying an individual, the method comprising:
- initiating, with a local identity server, a personalization of a partner-specific identification vehicle that identifies the individual based at least in part on an individual global unique identifier associated with the individual;
- 30 receiving, with the local identity server, a request for a service from the individual via a network;
- receiving, with the local identity server, consent and registration information from the individual via the network;

generating, with the local identity server, an identity confirmation that confirms an identity of the individual; and
outputting, with the local identity server, the identity confirmation to the network,

5 wherein the individual global unique identifier is generated from information derived from the registration information, and

 wherein the individual global unique identifier is not indicative of personally identifiable information of the individual.

10 12. The method of claim 11, further comprising:

 receiving, with a local partner server, the request for the service from the individual;

 outputting, with the local partner server, the consent and the registration information from the individual to the network;

15 receiving, with the local partner server, the identity confirmation via the network; and

 approving, with the local partner server, the request for the service from the individual based on the identity confirmation,

 wherein the local identity server and the local partner server communicate
20 with each other over the network.

 13. The method of claim 12, further comprising:

 receiving, with the local partner server, a first biometric template of the individual from the partner-specific identification vehicle that is assigned to the
25 individual;

 generating, with the local partner server, a second biometric template of the individual based on the registration information;

 outputting, with the local partner server, the first biometric template of the individual and the second biometric template of the individual to the network;

30 receiving, with the local identity server, the first biometric template and the second biometric template via the network;

 determining, with the local identity server, whether the first biometric template is associated with one of one or more legacy servers; and

outputting, with the local identity server, the first biometric template to the one of the one or more legacy servers via the network in response to determining that the first biometric template is associated with the one of the one or more legacy servers;

wherein the local identity server, the local partner server, and one or more
5 legacy servers communicate with each other via the network, and
wherein each of the one or more legacy servers includes a legacy database.

14. The method of claim 13, further comprising:

outputting, with the local identity server, the first biometric template to the
10 network;

receiving, with a global identity server, the first biometric template via the network;

translating, with the global identity server, the first biometric template into a biometric hash;

15 performing, with the global identity server, de-duplication to determine whether the biometric hash matches any other biometric hashes;

associating, with the global identity server, the biometric hash with the individual global unique identifier that is assigned to the individual in response to determining that the biometric hash matches a different biometric hash that is already
20 associated with the individual;

storing, with the global identity server, the biometric hash in a memory in response to associating the biometric hash with the individual global unique identifier; and

outputting, with the global identity server, the identity confirmation to the
25 network in response to associating the biometric hash with the individual global unique identifier.

15. The method of claim 13, further comprising:

translating, with the local identity server, the first biometric template into a
30 biometric hash;

performing, with the local identity server, de-duplication to determine whether the biometric hash matches any other biometric hashes;

associating, with the local identity server, the biometric hash with the individual global unique identifier that is assigned to the individual in response to

determining that the biometric hash matches a different biometric hash that is already associated with the individual;

storing, with the local identity server, the biometric hash in a memory in response to associating the biometric hash with the individual global unique identifier;

5 and

outputting, with the local identity server, the identity confirmation to the network in response to associating the biometric hash with the individual global unique identifier.

10 16. The method of claim 12, further comprising:

receiving, with the local partner server, a first biometric template of the individual from the partner-specific identification vehicle that is assigned to the individual;

15 generating, with the local partner server, a second biometric template of the individual based on the registration information;

outputting, with the local partner server, the first biometric template of the individual and the second biometric template of the individual to the network;

generating, with the local identity server, a biometric hash based on the second biometric template;

20 outputting, with the local identity server, the first biometric template and the biometric hash to the network;

receiving, with a global identity server, the first biometric template and the biometric hash via the network;

25 translating, with the global identity server, the first biometric template into a second biometric hash;

performing, with the global identity server, de-duplication to determine whether the biometric hash and the second biometric hash match any other biometric hashes;

30 associating, with the global identity server, the biometric hash and the second biometric hash with the individual global unique identifier that is assigned to the individual in response to determining that the biometric hash and the second biometric hash match a different biometric hash that is already associated with the individual;

storing, with the global identity server, the biometric hash and the second biometric hash in a memory in response to associating the biometric hash and the second biometric hash with the individual global unique identifier; and

5 outputting, with the global identity server, the identity confirmation to the network in response to associating the biometric hash and the second biometric hash with the individual.

17. The method of claim 12, further comprising:

10 receiving, with the local partner server, a first biometric template of the individual from the partner-specific identification vehicle that is assigned to the individual;

 generating, with the local partner server, a second biometric template of the individual based on the registration information;

15 outputting, with the local partner server, the first biometric template of the individual and the second biometric template of the individual to the network;

 generating, with the local identity server, a biometric hash based on the second biometric template;

 translating, with the local identity server, the first biometric template into a second biometric hash;

20 performing, with the local identity server, de-duplication to determine whether the biometric hash and the second biometric hash match any other biometric hashes;

 associating, with the local identity server, the biometric hash and the second biometric hash with the individual global unique identifier that is assigned to the individual in response to determining that the biometric hash and the second biometric
25 hash match a different biometric hash that is already associated with the individual;

 storing, with the local identity server, the biometric hash and the second biometric hash in a memory in response to associating the biometric hash and the second biometric hash with the individual global unique identifier; and

 outputting, with the local identity server, the identity confirmation to the local
30 partner server to the network in response to associating the biometric hash and the second biometric hash with the individual global unique identifier.

18. The method of claim 12, further comprising:

generating, with the local partner server, a biometric template of the individual based on the registration information; and
outputting, with the local partner server, the biometric template of the individual to the network.

5

19. The method of claim 18, further comprising:
receiving, with the local identity server, the biometric template via the network;
generating, with the local identity server, a biometric hash based on the
10 biometric template;
performing, with the local identity server, de-duplication to determine whether the biometric hash matches any other biometric hashes;
associating, with the local identity server, the biometric hash with the individual global unique identifier that is assigned to the individual in response to
15 determining that the biometric hash matches a different biometric hash that is already associated with the individual;
storing, with the local identity server, the biometric hash in a memory in response to associating the biometric hash with the individual global unique identifier;
and
20 outputting, with the local identity server, the identity confirmation to the network in response to associating the biometric hash with the individual global unique identifier.

20. The method of claim 18, further comprising:
25 receiving, with the local identity server, the biometric template via the network;
generating, with the local identity server, a biometric hash based on the biometric template;
outputting, with the local identity server, the biometric hash to the network;
30 receiving, with a global identity server, the biometric hash via the network;
performing, with the global identity server, de-duplication to determine whether the biometric hash matches any other biometric hashes;
associating, with the global identity server, the biometric hash with the individual global unique identifier that is assigned to the individual in response to

determining that the biometric hash matches a different biometric hash that is already associated with the individual;

storing, with the global identity server, the biometric hash in a memory in response to associating the biometric hash with the individual global unique identifier;

5 and

outputting, with the global identity server, the identity confirmation to the local partner server to the network in response to associating the biometric hash with the individual global unique identifier.

10 21. 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, the set of operations comprising:

initiating a personalization of a partner-specific identification vehicle that identifies an individual based at least in part on an individual global unique identifier

15 associated with the individual;

receiving a request for a service from the individual via a network;

receiving consent and registration information from the individual via the network;

generating an identity confirmation that confirms an identity of the individual;

20 and

outputting the identity confirmation to the network,

wherein the individual global unique identifier is generated from information derived from the registration information, and

25 wherein the individual global unique identifier is not indicative of personally identifiable information of the individual.

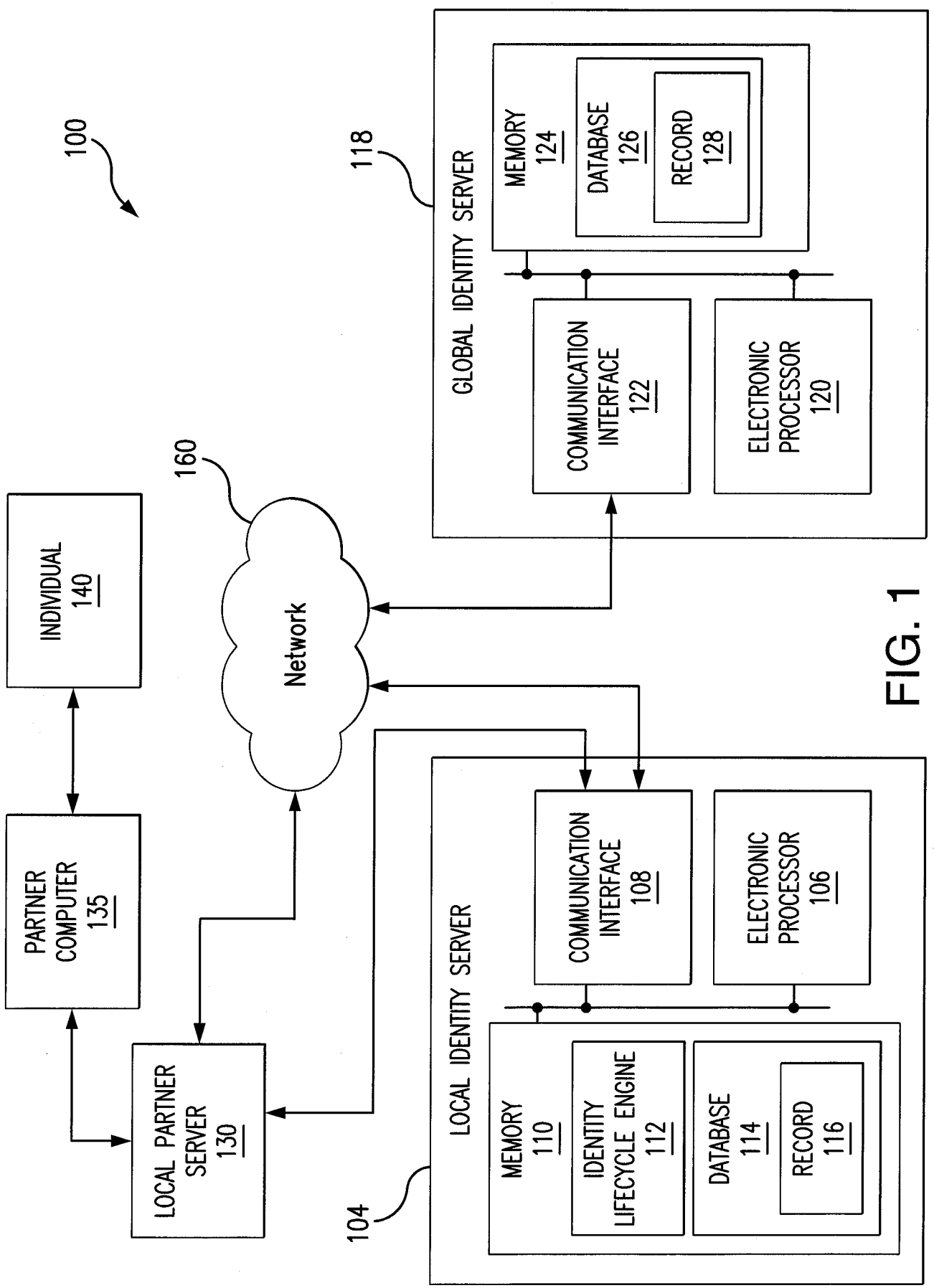
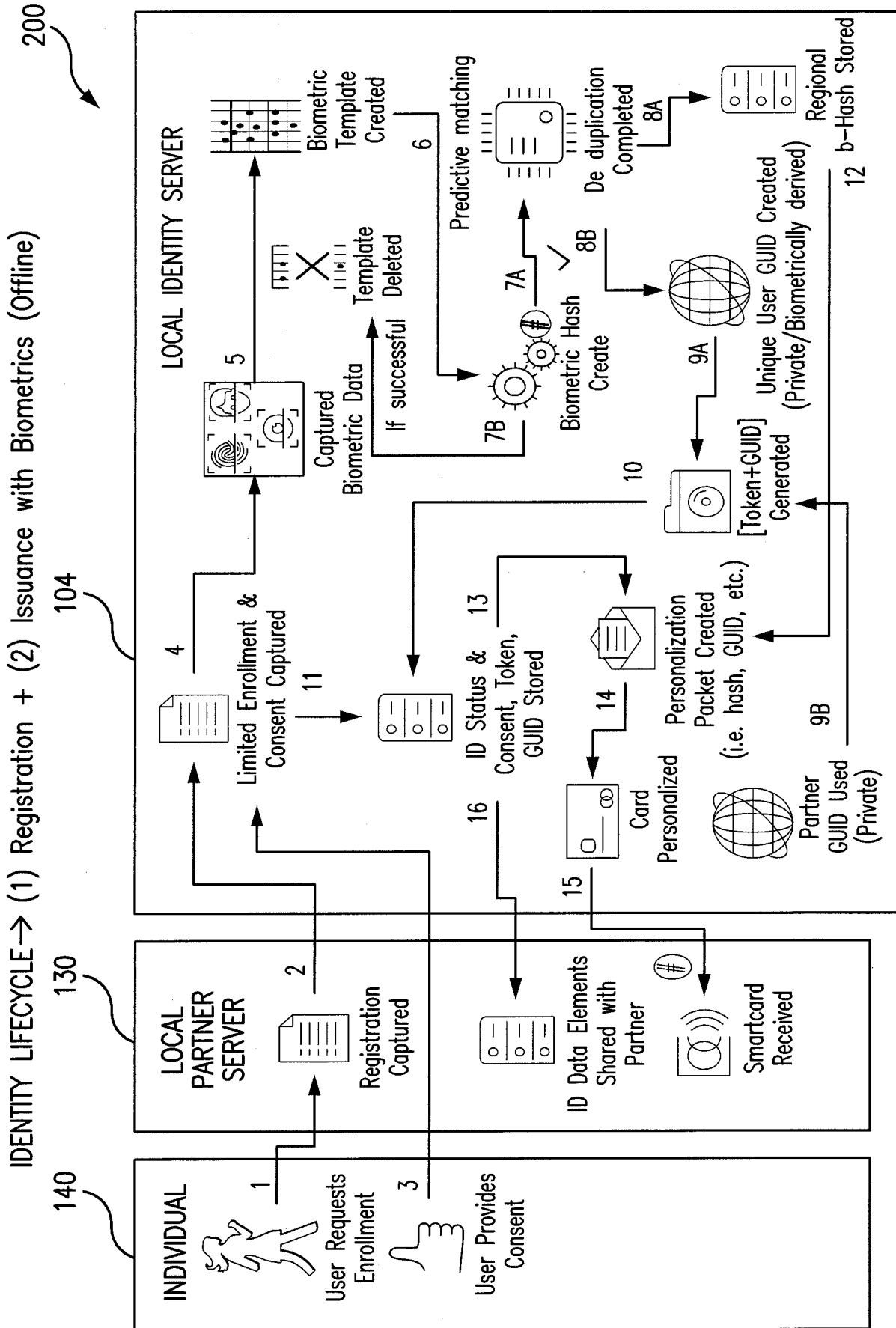
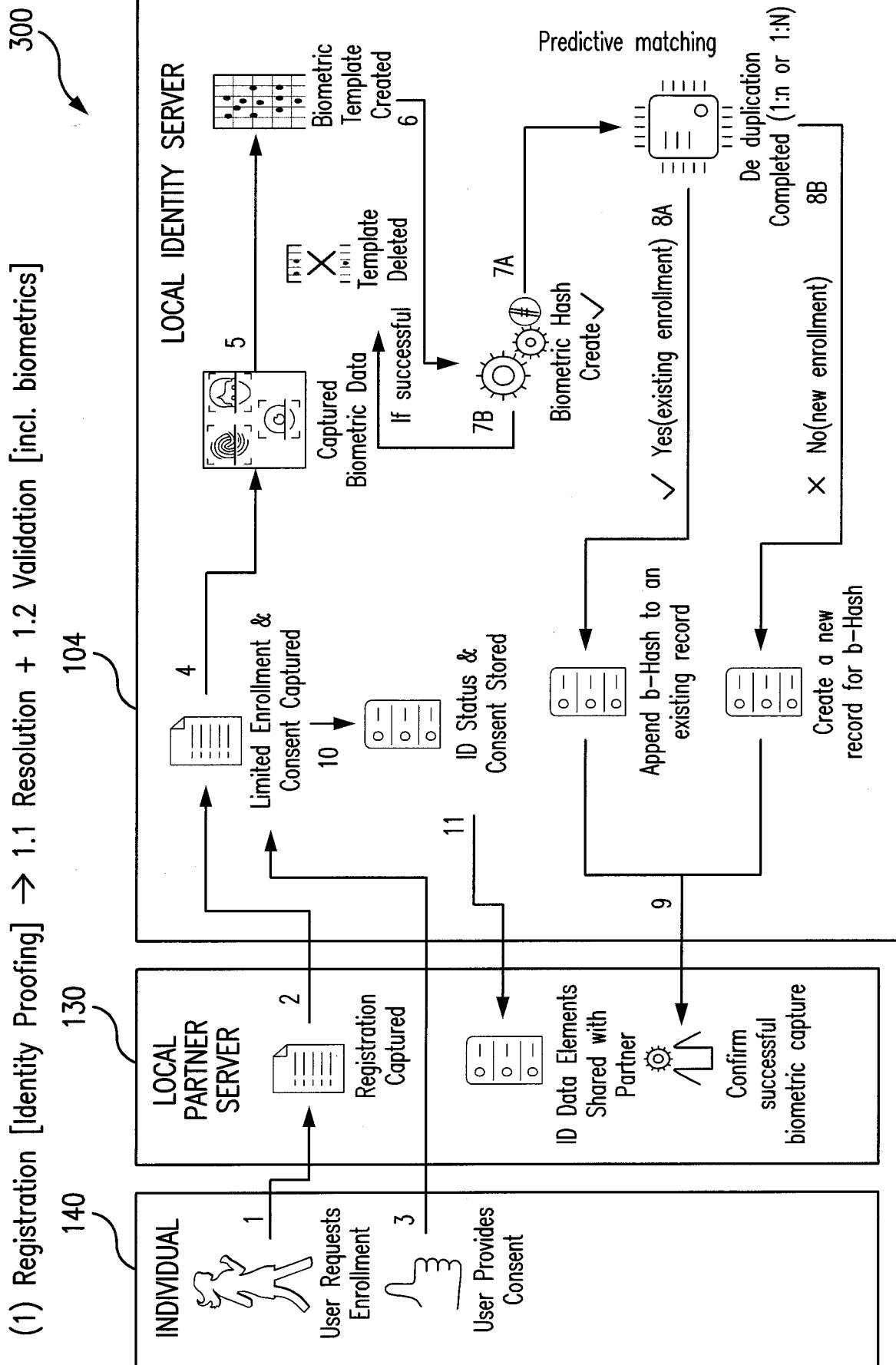


FIG. 1

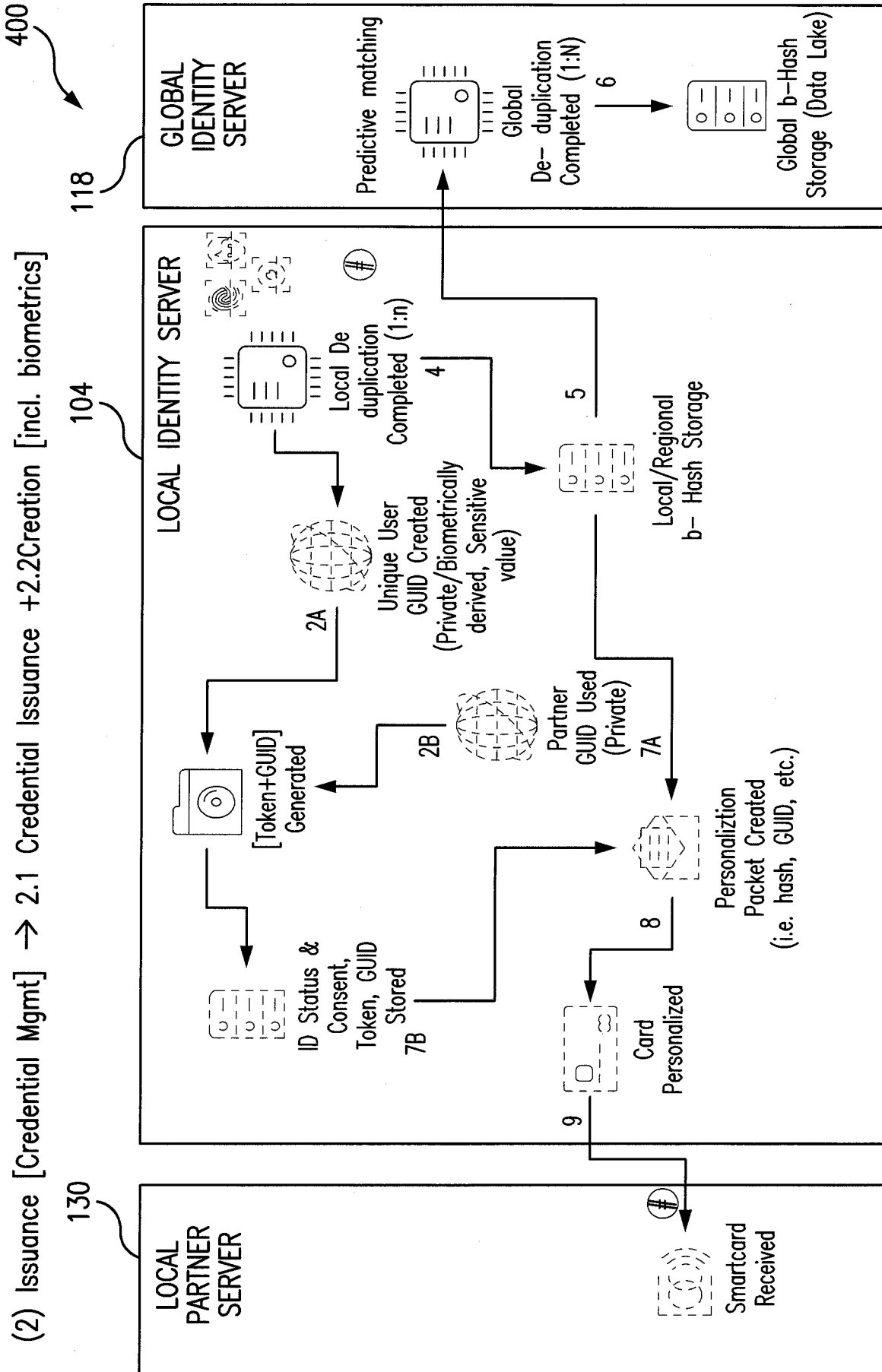


SCENARIO A: REGISTRATION+BIOMETRIC ENROLLMENT OF AN INDIVIDUAL INTO AN AID PROGRAM

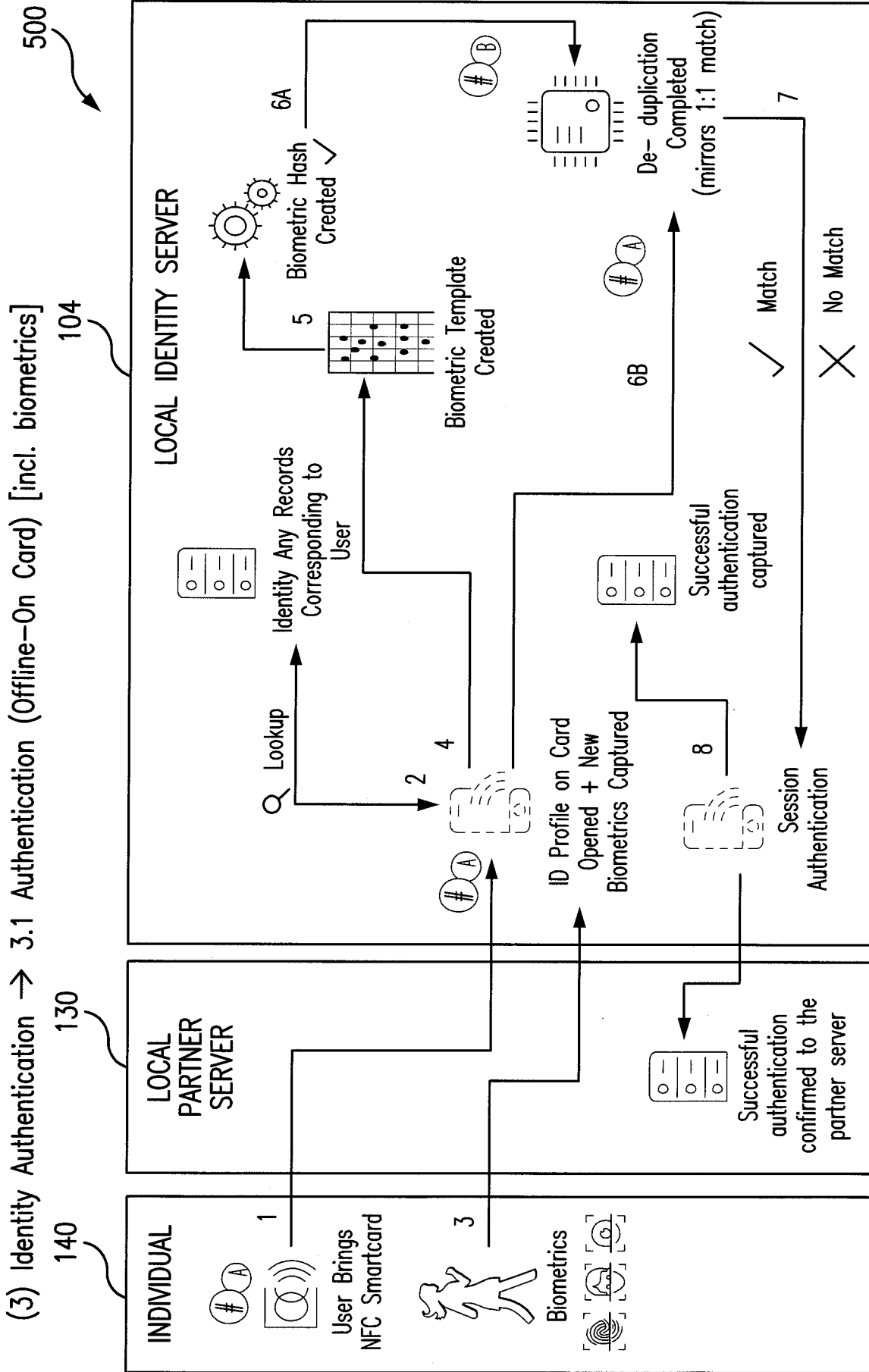
FIG. 2



USE CASE#1: AN INDIVIDUAL REGISTERS FOR A BIOMETRICALLY VERIFIED IDENTITY FOR EXAMPLE $\rightarrow$ AN INDIVIDUAL ENROLLS INTO A LIVELIHOODS PROGRAM WITH SAVE THE CHILDREN **FIG. 3**



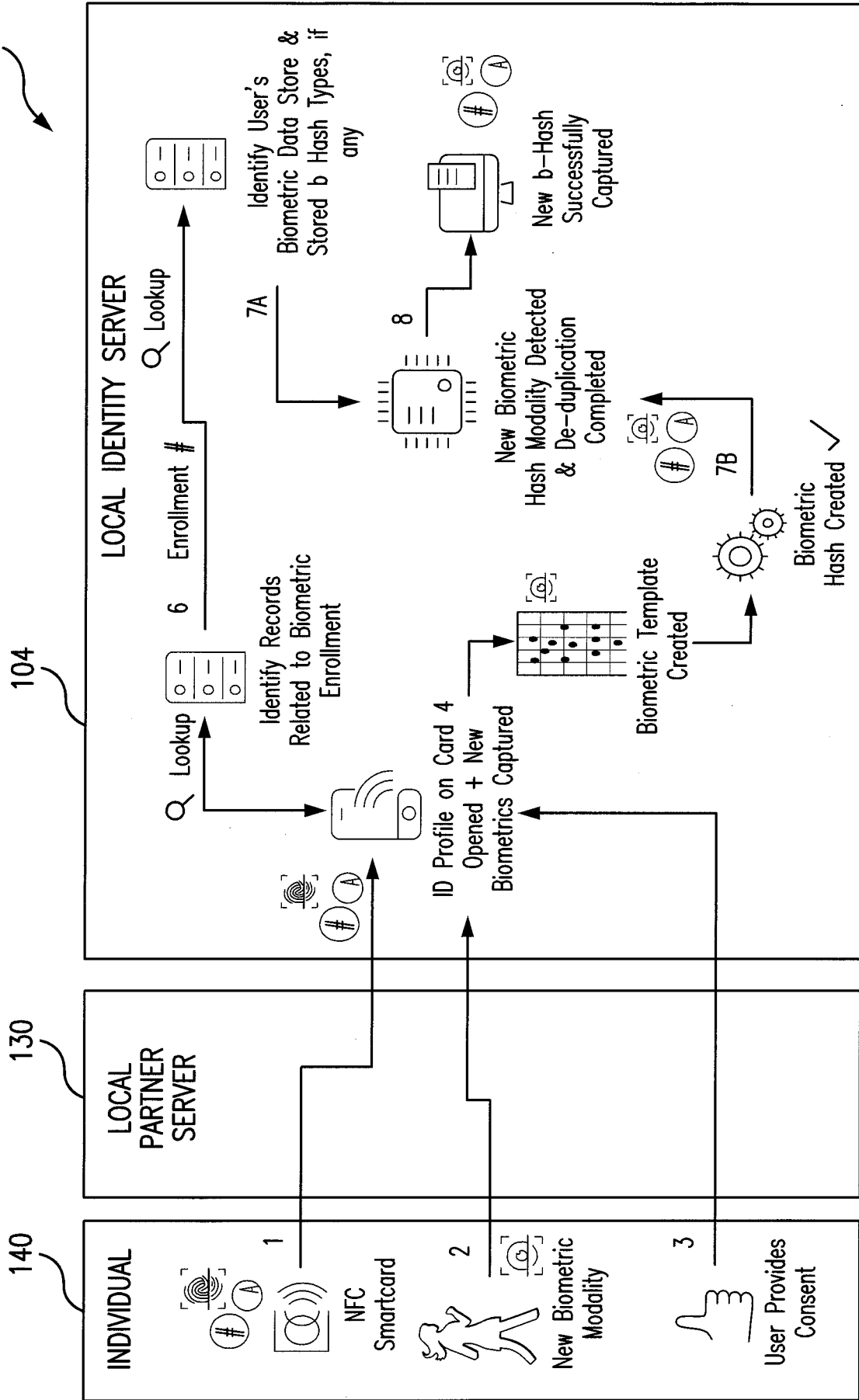
USE CASE#2: REGISTERED INDIVIDUAL RECEIVES A BIOMETRICALLY VERIFIED IDENTITY SMARTCARD
FOR EXAMPLE → BENEFICIARY RECEIVES AN ID CREDENTIAL UPON SUCCESSFUL ENROLLMENT [ID PROFILE CREATED] **FIG. 4**



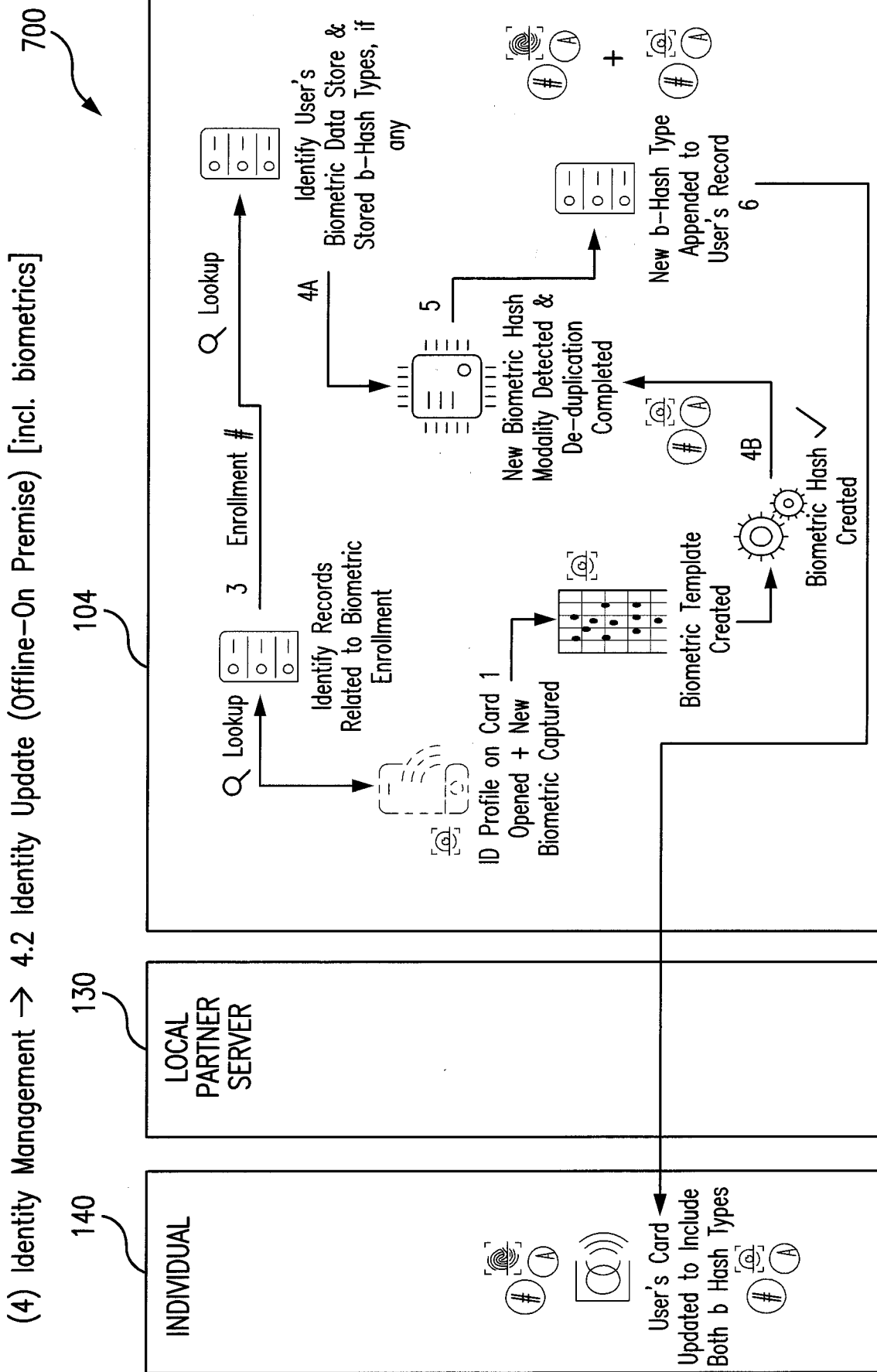
USE CASE #3: AN INDIVIDUAL PROVES THAT S/HE IS THE OWNER OF THE ID CREDENTIAL
 FOR EXAMPLE → A CAREGIVER PROVES IDENTITY ON CARD ONLY FOR LOW VALUE TRANSACTIONS → REDEMPTION
 OF A VOUCHER AT A PHARMACY [OR WHEN BIOMETRIC DATA STORAGE IS NOT FEASIBLE]

FIG. 5

(4) Identity Management → 4.1 Identity Maintenance (Offline-On Premise) [incl. biometrics]



USE CASE #5: A 2ND BIOMETRIC MODALITY FOR THE SAME & UNIQUE INDIVIDUAL IS CAPTURED FOR EXAMPLE → A FARMER REGISTERED WITH OXFAM (BY FINGERPRINT) REGISTERS WITH RED CROSS (USING IRIS) **FIG. 6**

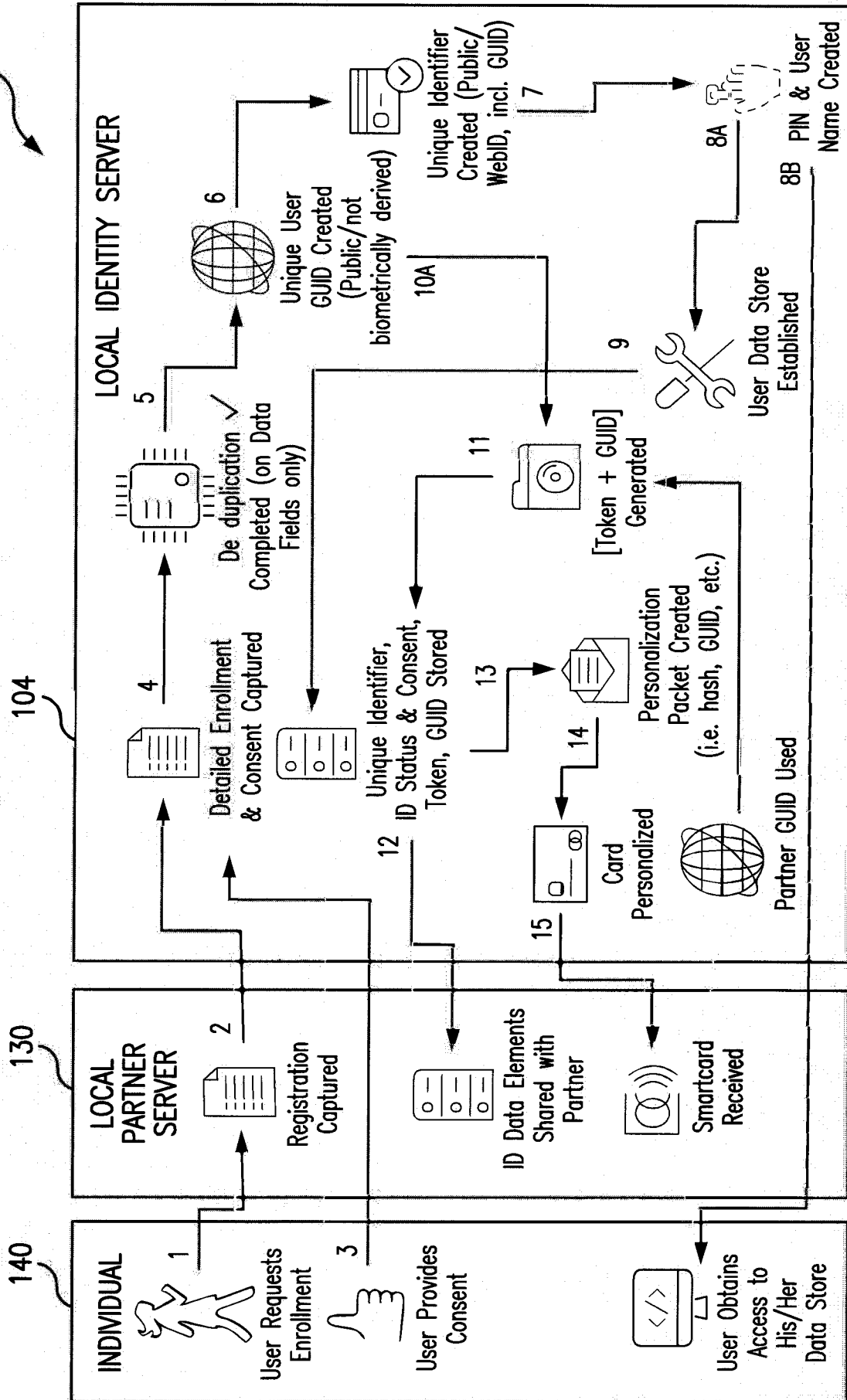


USE CASE #6: A REGISTERED INDIVIDUAL'S ID PROFILE IS UPDATED WITH 2ND BIOMETRIC MODALITY
FOR EXAMPLE → A FARMER REGISTERED WITH OXFAM & RED CROSS IS NOW RECOGNIZED AS ONE

FIG. 7

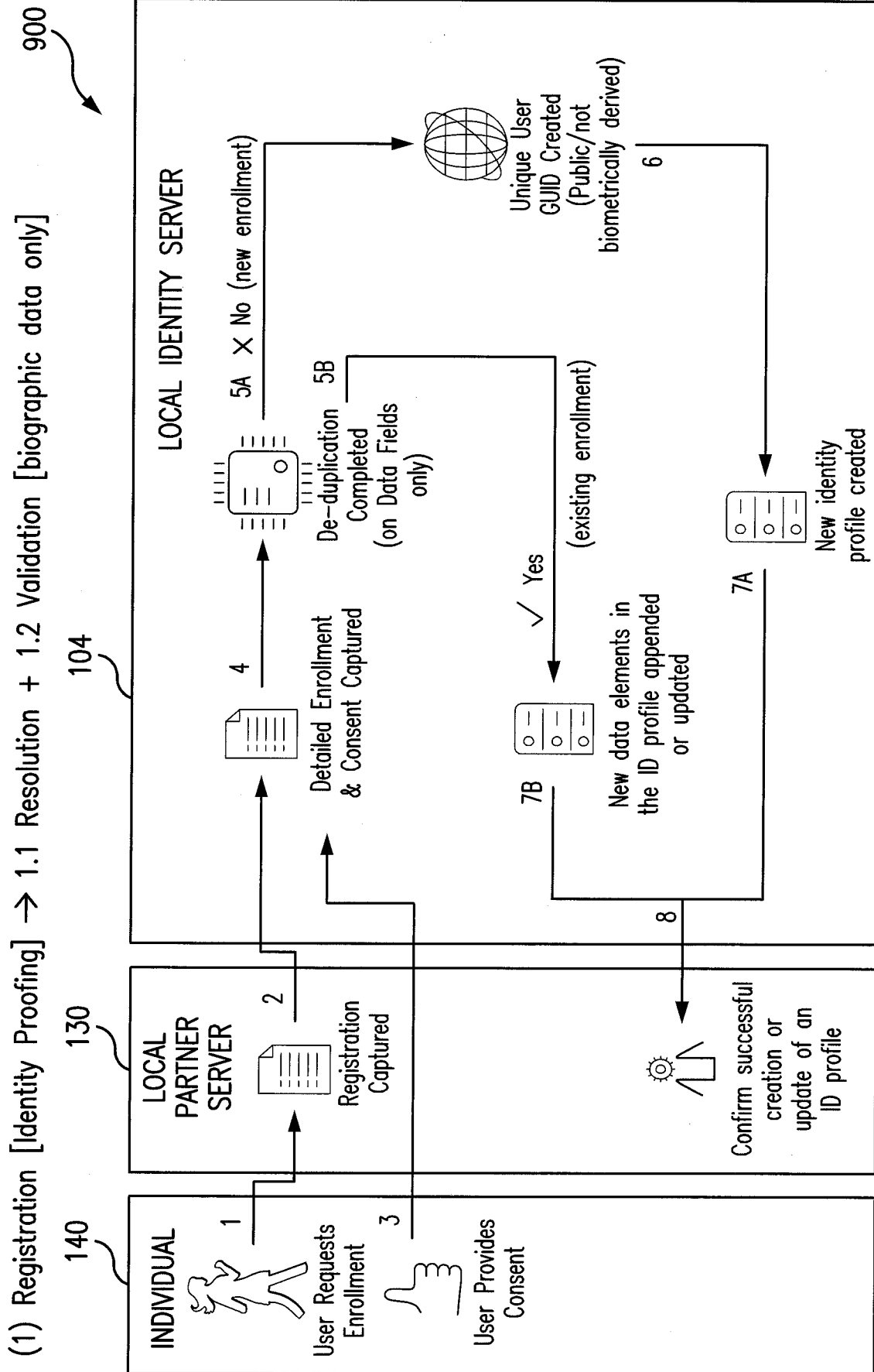
IDENTITY LIFECYCLE → (1) Registration + (2) Issuance without Biometrics (Offline)

800



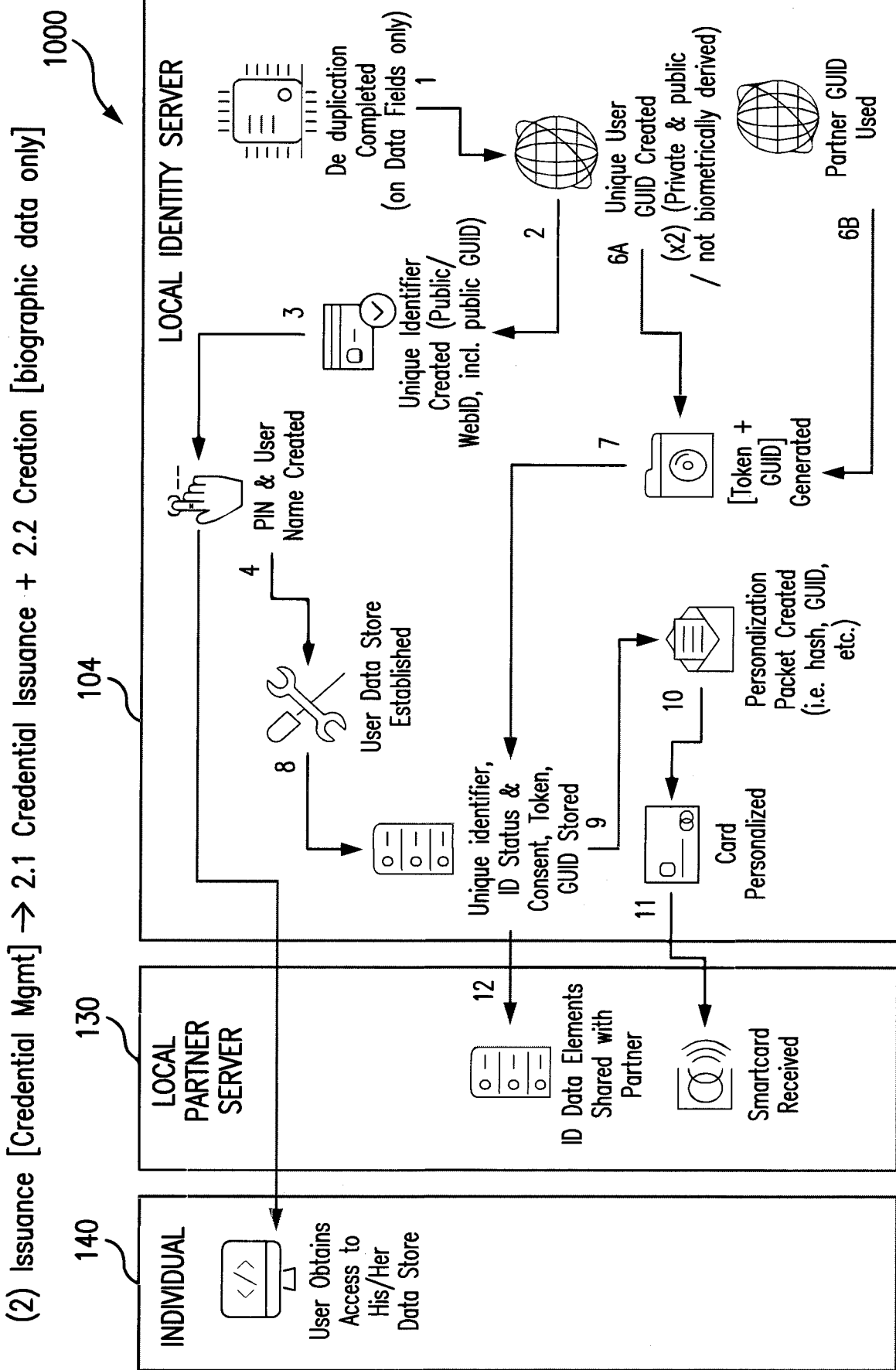
SCENARIO B: NON-BIOMETRIC REGISTRATION OF INDIVIDUAL INTO AN AID PROGRAM

FIG. 8



USE CASE #7: AN INDIVIDUAL REGISTERS FOR AN ID PROFILE (ACCOUNT) WITH AN NGO
FOR EXAMPLE → AN INDIVIDUAL ENROLLS INTO A LIVELIHOODS PROGRAM WITH SAVE THE CHILDREN

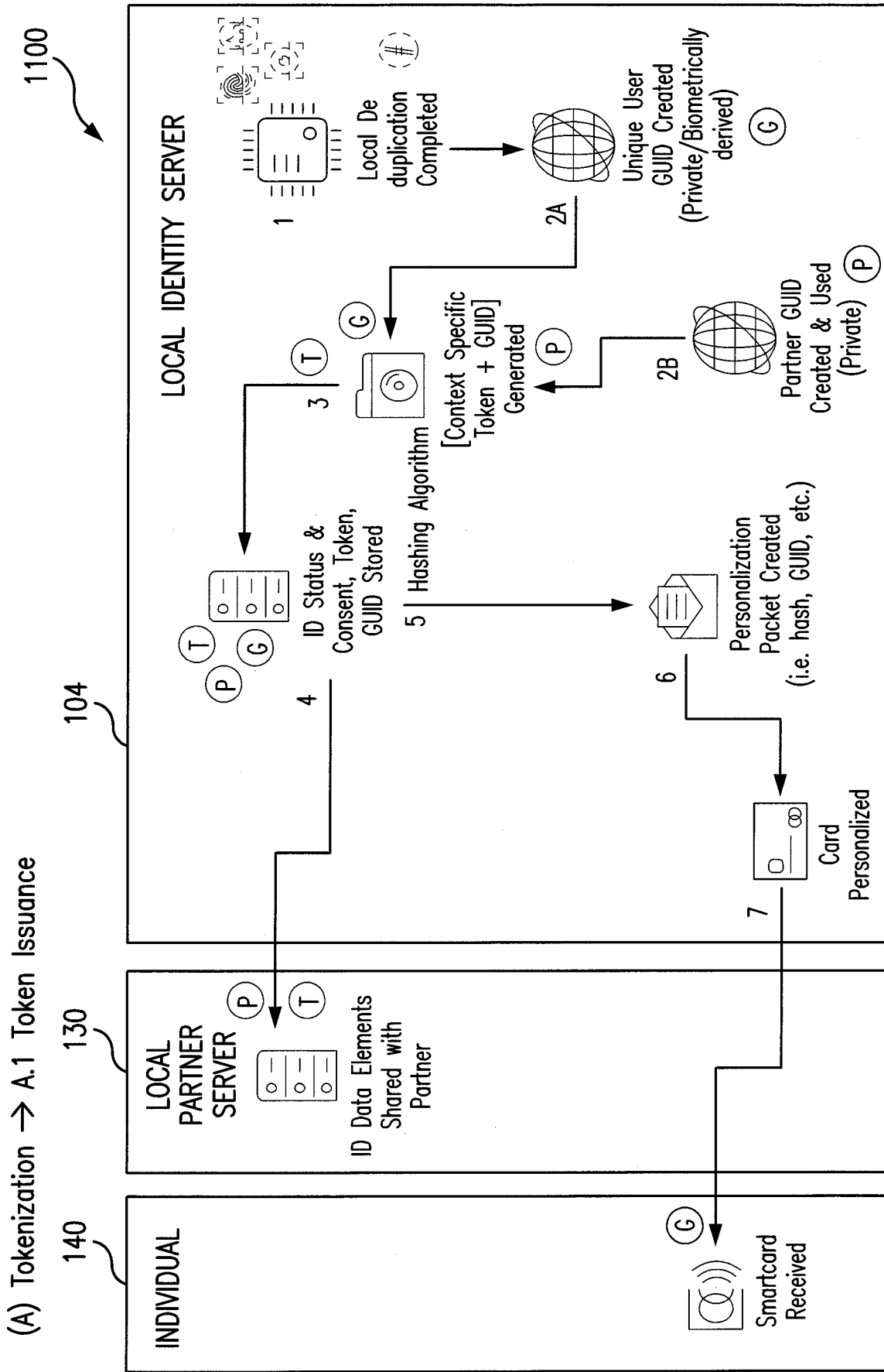
FIG. 9



USE CASE #8: REGISTERED INDIVIDUAL RECEIVES AN ID ACCOUNT SMARTCARD

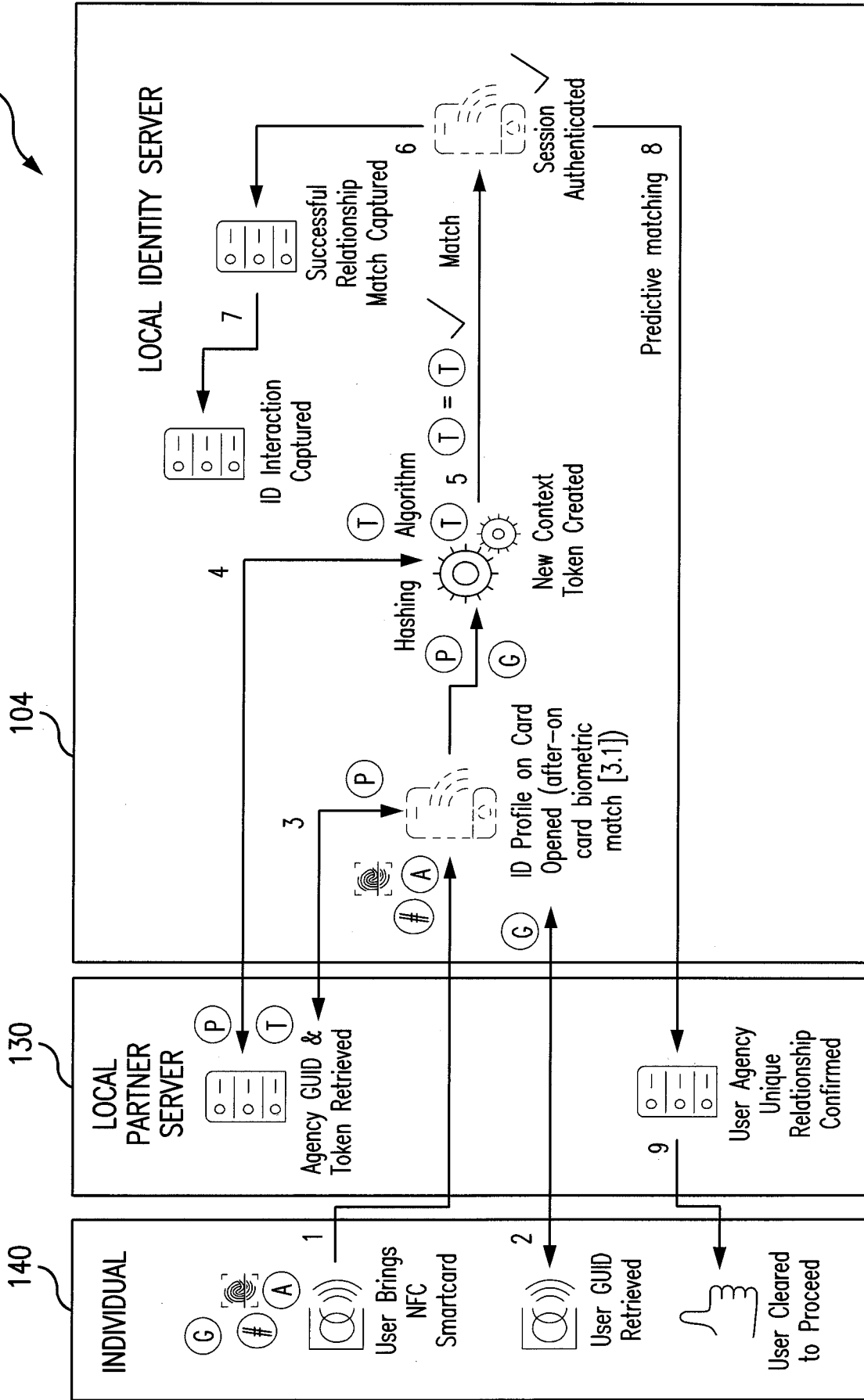
FOR EXAMPLE → BENEFICIARY RECEIVES AN ID CREDENTIAL UPON SUCCESSFUL REGISTRATION [ID PROFILE CREATED]

FIG. 10



USE CASE #9: A TOKEN REPRESENTING A RELATIONSHIP BETWEEN INDIVIDUAL AND NGO #1 IS ISSUED FOR EXAMPLE → A UNIQUE TOKEN IS CREATED ONLY FOR TRANSACTIONS BETWEEN AN INDIVIDUAL & RED CROSS **FIG. 11**

(A) Tokenization → A.2 Token Match Successful

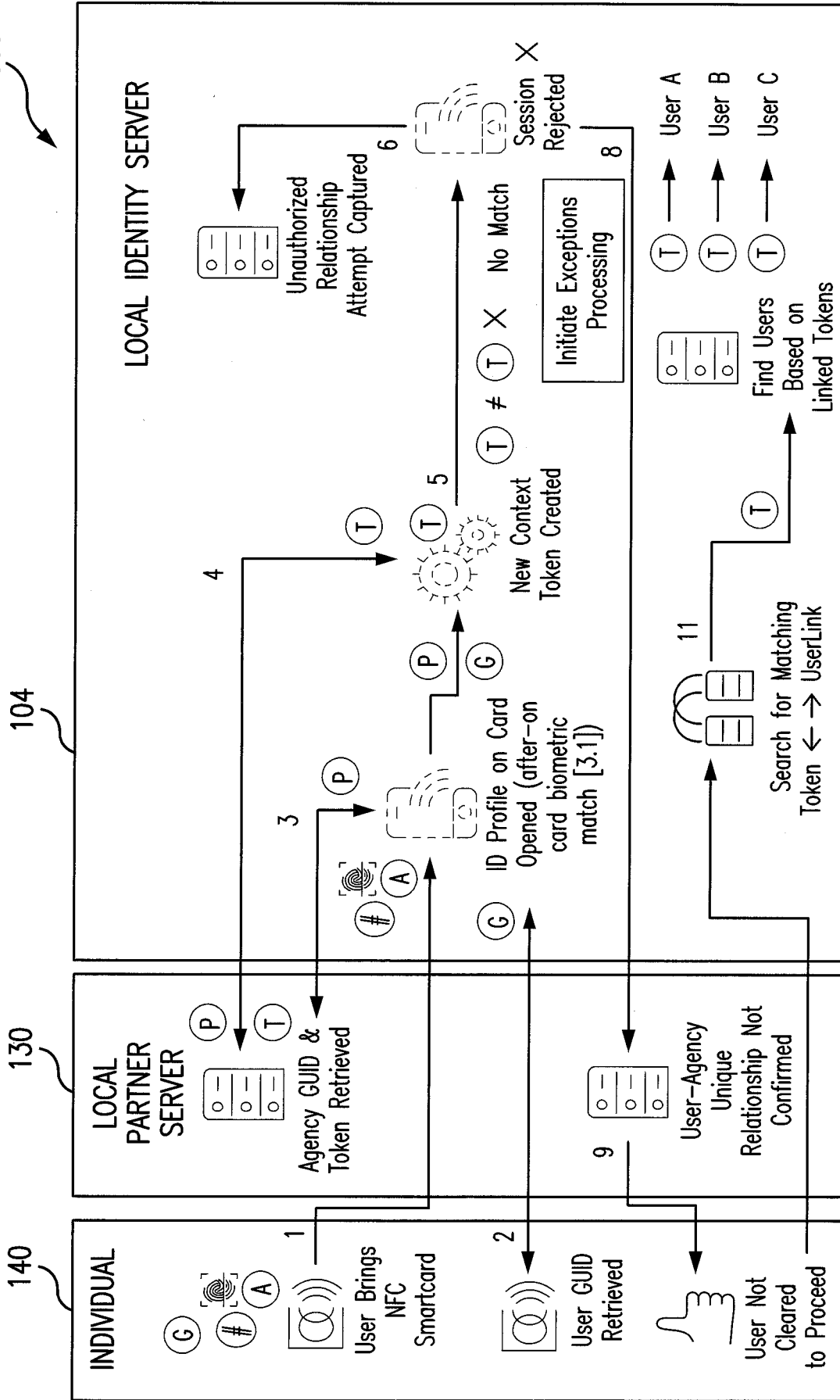


USE CASE #10: A NEW TOKEN CREATED DURING AN INTERACTION IS MATCHED TO A DESIGNATED TOKEN

FOR EXAMPLE → A FARMER'S CARD IS USED TO CREATE A NEW TOKEN THAT MATCHES WHAT RED CROSS HAS ON FILE

FIG. 12

(A) Tokenization → A.2 Token Match Not Successful



USE CASE #11: A NEW TOKEN CREATED DURING AN INTERACTION IS MATCHED TO A DESIGNATED TOKEN FOR EXAMPLE → A FARMER USES HIS CARD TO PRETEND THAT S/HE IS SOMEONE ELSE (GUID MISMATCH)

FIG. 13

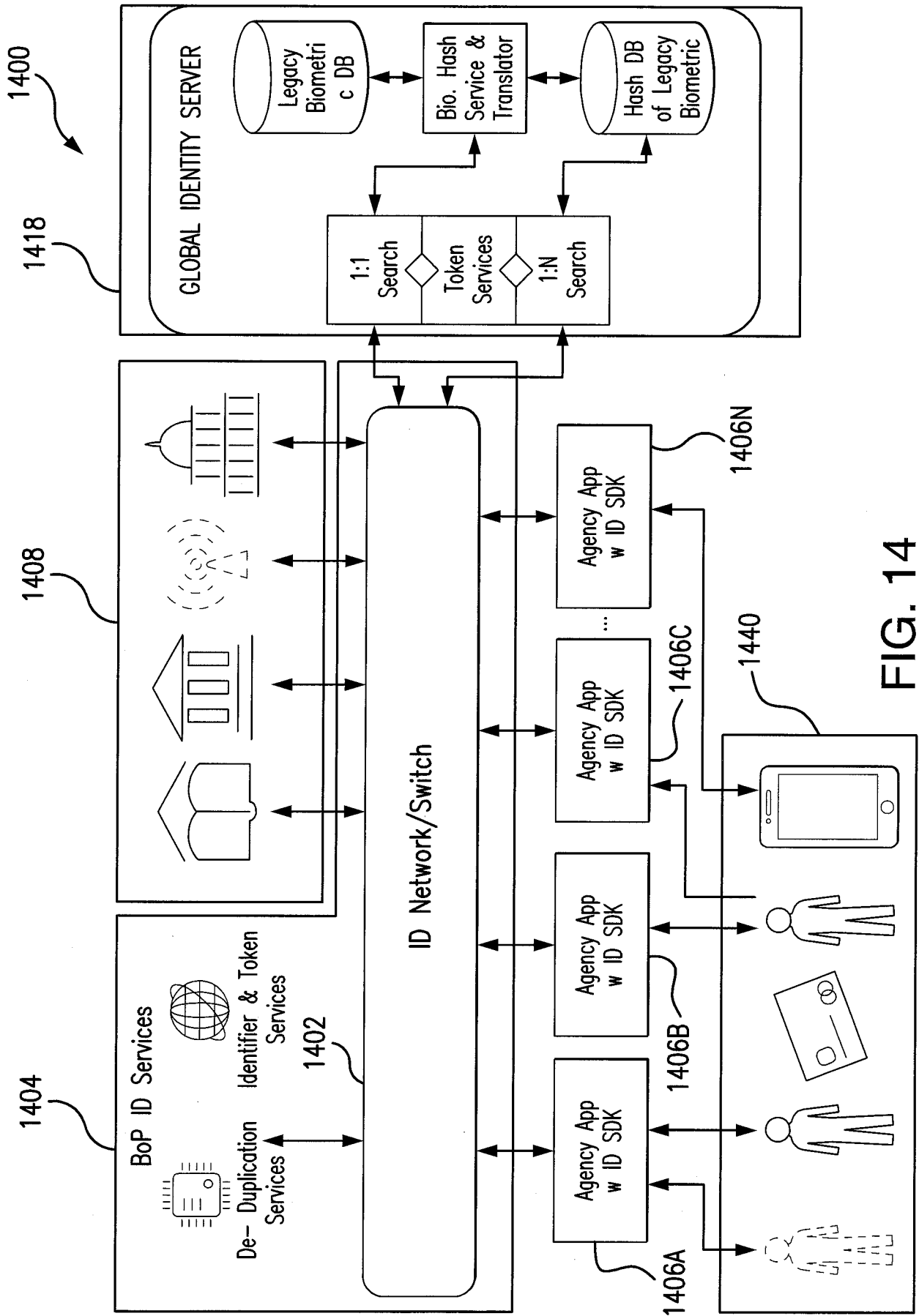
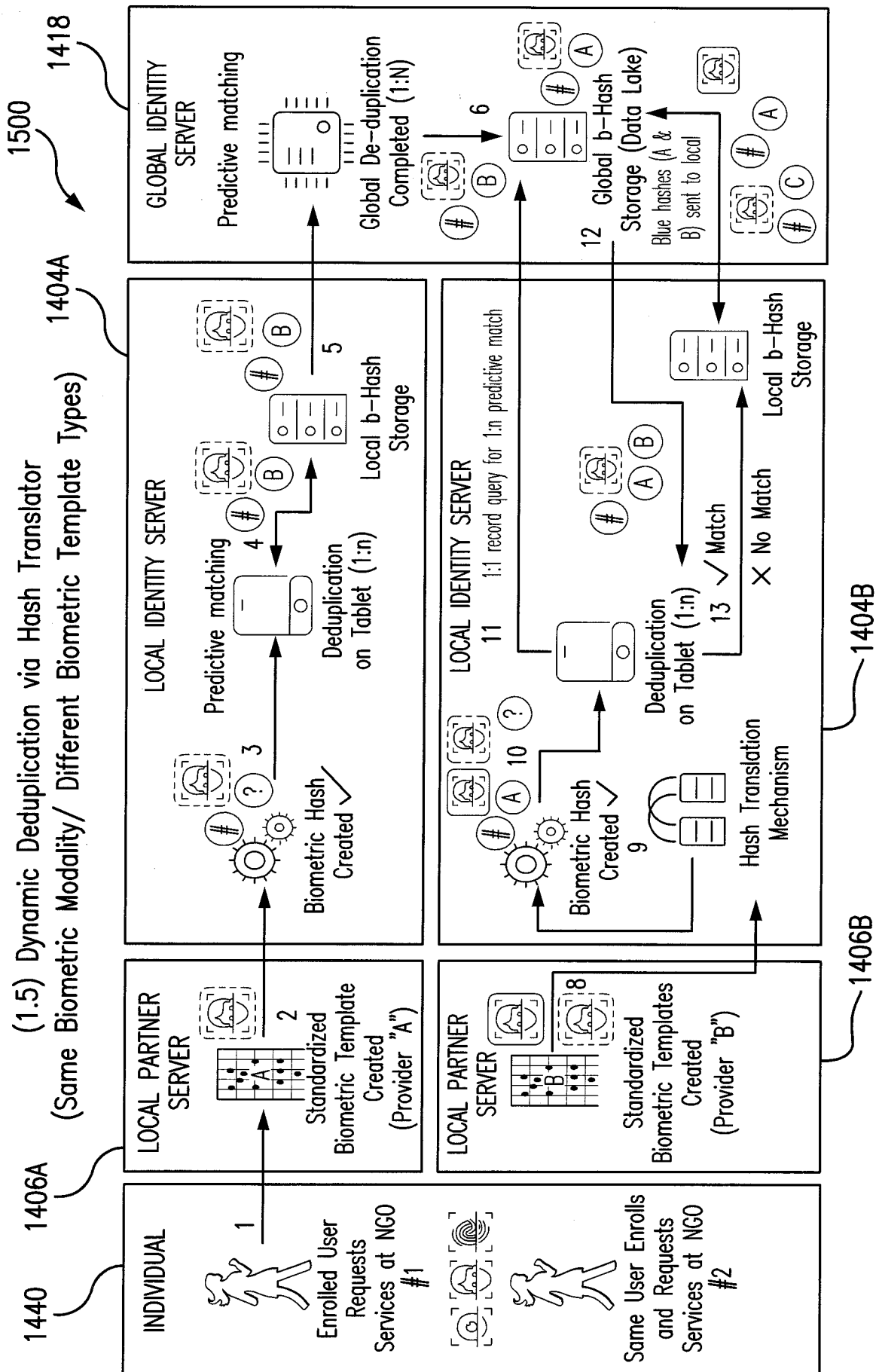
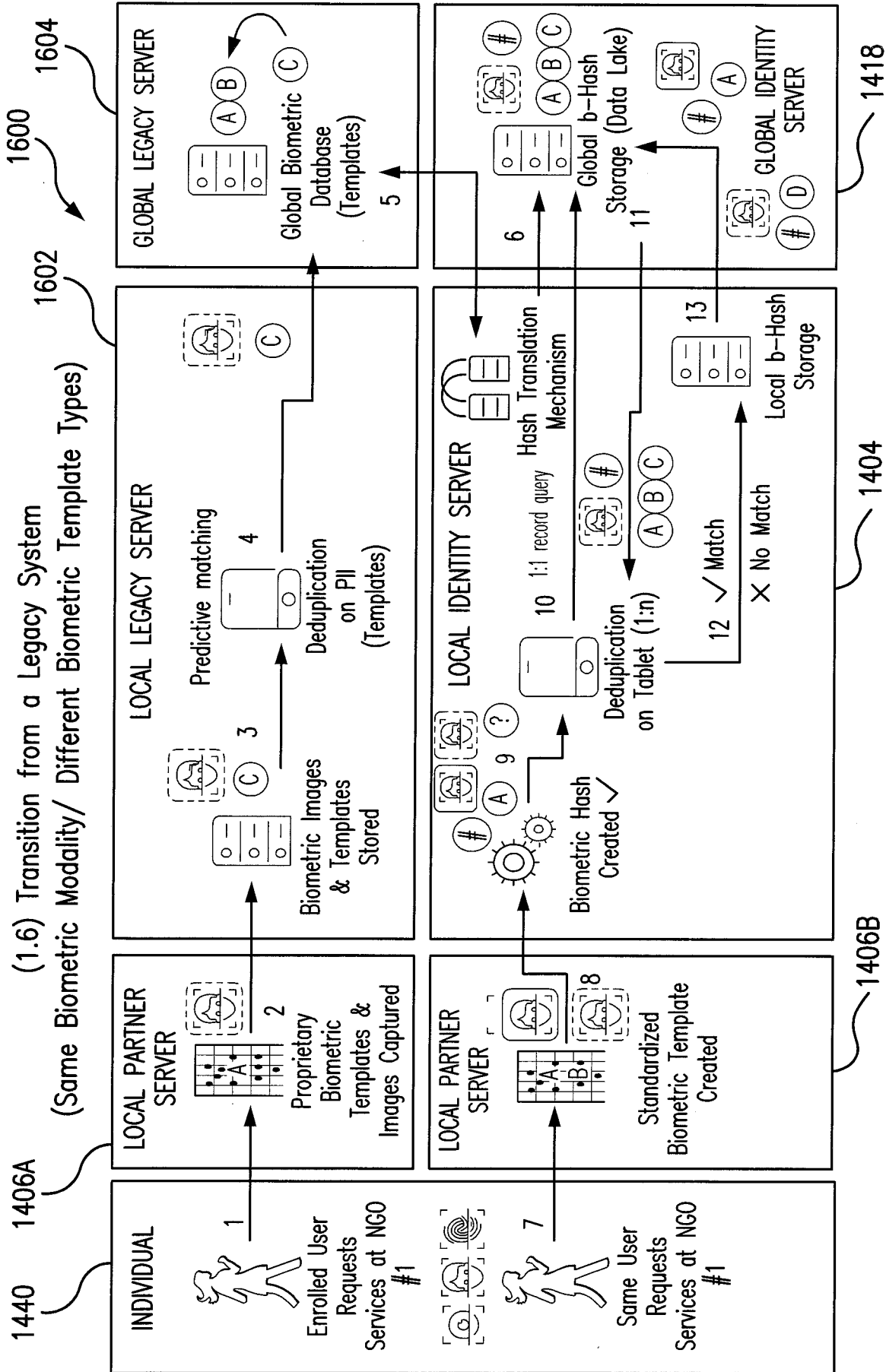


FIG. 14



SCENARIO A DEDUPLICATION OF A NEW FACE B-HASH AGAINST EXISTING FACE HASHES STORED

FIG. 15



SCENARIO B: DEDUPLICATION OF A NEW FACE B-HASH AGAINST A LEGACY BIOMETRIC DATABASE

FIG. 16

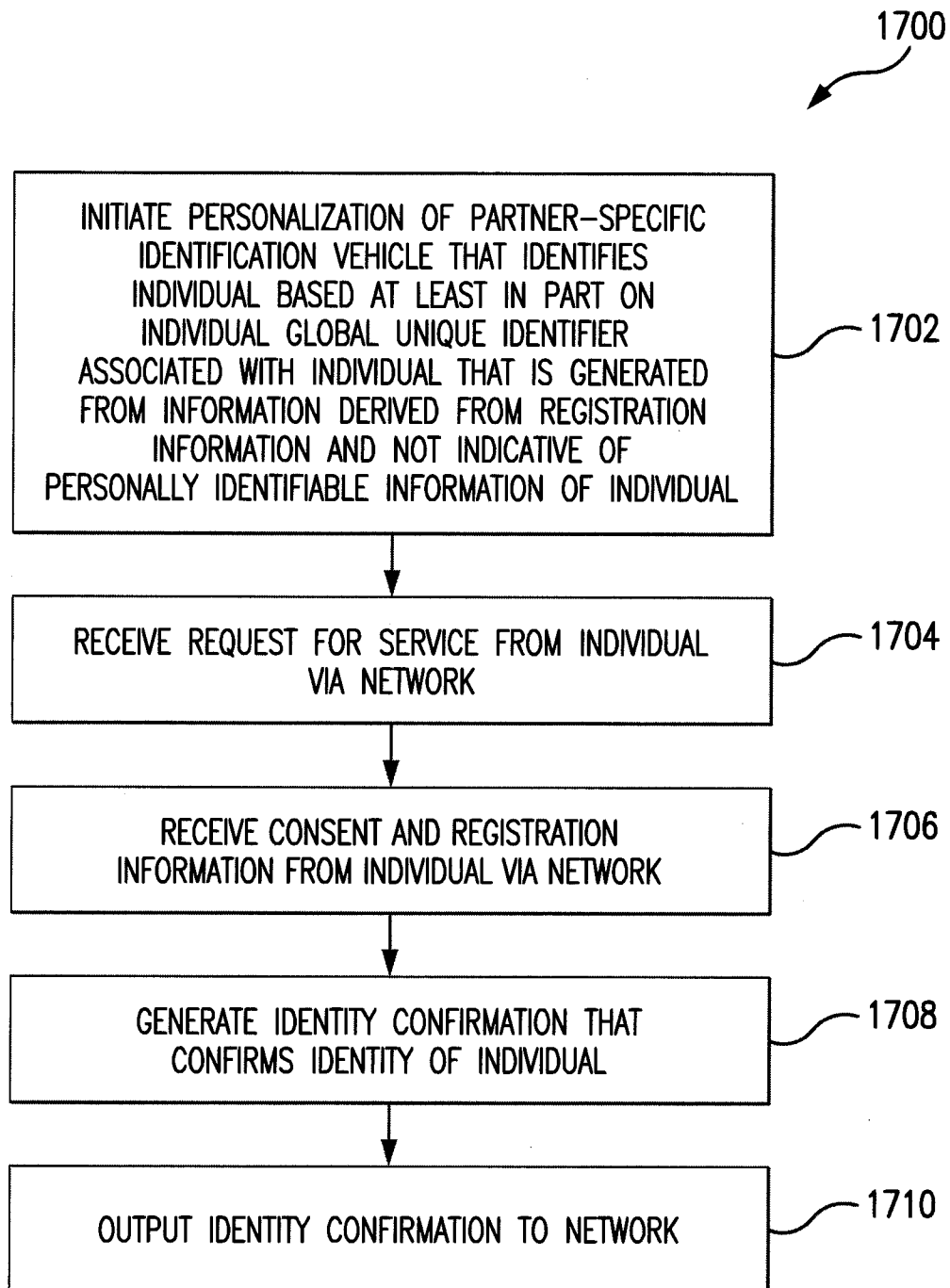


FIG. 17

A. CLASSIFICATION OF SUBJECT MATTER**H04L 29/06(2006.01)i, H04L 9/32(2006.01)i, G06F 21/32(2013.01)i**

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)

H04L 29/06; G06F 12/14; G06F 21/32; G06F 21/60; H04L 9/32

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: identification vehicle, global unique identifier, identity, registration

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2018-222211 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 06 December 2018 paragraphs [0031], [0055]-[0074], [0084]; and figures 1-2	1-21
Y	WO 2018-001831 A1 (ZWIPE AS) 04 January 2018 page 14, lines 2-15	1-21
Y	US 2017-0142102 A1 (FUJITSU LIMITED) 18 May 2017 paragraphs [0063]-[0064]	4-10, 14-20
A	US 10142333 B1 (WELLS FARGO BANK, N.A.) 27 November 2018 column 5, line 43 - column 19, line 49; and figures 1-6	1-21
A	KR 10-2017-0107409 A (SUPREMA ID INC.) 25 September 2017 paragraphs [0028]-[0197]; and figures 1-9	1-21



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

25 March 2020 (25.03.2020)

Date of mailing of the international search report

25 March 2020 (25.03.2020)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

KIM, Sung Hee

Telephone No. +82-42-481-3516



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/064125

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2018-222211 A1	06/12/2018	None	
WO 2018-001831 A1	04/01/2018	CN 109478213 A EP 3479278 A1 GB 2553165 A JP 2019-525310 A KR 10-2019-0021368 A US 2019-0220582 A1	15/03/2019 08/05/2019 28/02/2018 05/09/2019 05/03/2019 18/07/2019
US 2017-0142102 A1	18/05/2017	JP 2017-092857 A US 10291611 B2	25/05/2017 14/05/2019
US 10142333 B1	27/11/2018	US 10193884 B1	29/01/2019
KR 10-2017-0107409 A	25/09/2017	KR 10-1768213 B1 US 2017-0264429 A1	31/08/2017 14/09/2017