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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
06 September 2019 (06.09.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/168782 A1

(51) International Patent Classification:
G07G 1/14 (2006.01) *H04W 4/18* (2009.01)
H04W 4/06 (2009.01)

(21) International Application Number:
PCT/US2019/019397

(22) International Filing Date:
25 February 2019 (25.02.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/635,704 27 February 2018 (27.02.2018) US

(71) Applicant *(for all designated States except US)*: **THIN FILM ELECTRONICS ASA** [NO/NO]; Henrik Ibsens Gate 100, N-0255 Oslo (NO).

(72) Inventor; and

(71) Applicant *(for US only)*: **ASHKENAZI, Zvika** [US/US]; 846 Alderbrook Ln., Cupertino, CA 95014 (US).

(74) Agent: **FORTNEY, Andrew, D.** et al.; Central California IP Group, P.C., 377 W. Fallbrook Avenue, Suite 205, Fresno, CA 93711 (US).

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

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

(54) Title: SYSTEM AND METHOD FOR MANAGING WIRELESS TAG FUNCTIONALITY

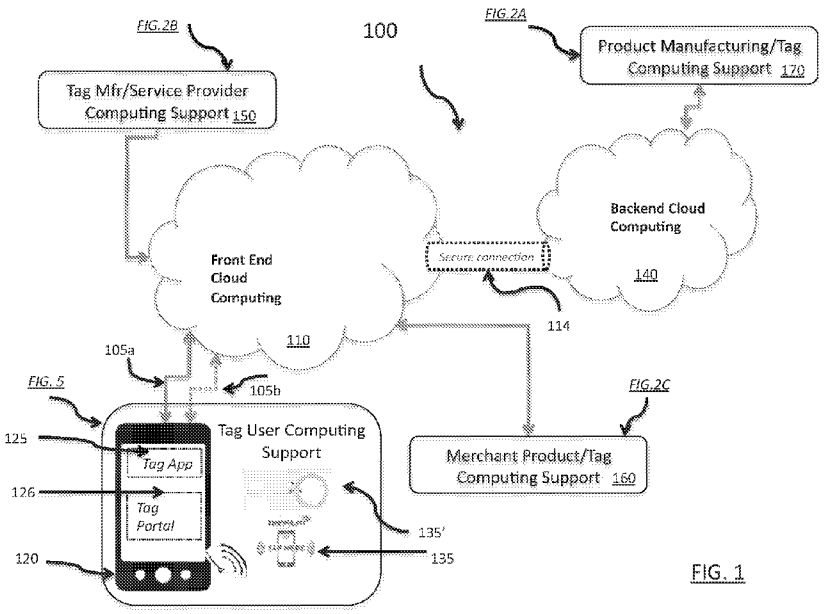

FIG. 1

(57) Abstract: Wireless tags and related mobile applications include a combination of both public and hidden functionality. Tag hidden features can be unlocked with a customized mobile application coordinating with a server through two separate channels. Conversely hidden features of a mobile application are made accessible through reading coded wireless tags. The combination of tag and mobile application afford a simplified and convenient form of two factor authentication.

[Continued on next page]

WO 2019/168782 A1

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

Published:

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

SYSTEM AND METHOD FOR MANAGING WIRELESS TAG FUNCTIONALITY

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application claims the benefit of U.S. Provisional Pat. Appl. No. 62/635,704, filed on February 27, 2018, incorporated herein by reference as if fully set forth herein.

FIELD OF THE INVENTION

[0002] The present invention generally relates to the field(s) of managing interactions between users, wireless tags and mobile applications. More specifically, embodiments of the present invention pertain to computer-implemented methods for authenticating users and unlocking functions of wireless tags and related applications operating on mobile computing devices.

DISCUSSION OF THE BACKGROUND

[0003] Wireless near field communication (NFC) and radio frequency (RF) security and/or identification tags are used to digitally track and manage products by their manufacturers and distributors. Such wireless tags are often associated with a product by a manufacturer of the tag, and subsequently shipped to the manufacturer or distributor of the product.

[0004] In some commercial applications, it may be desirable to obscure part of the functionality of a tag to end-users unless they satisfy particular merchant criteria, or are using an authorized merchant application. For example, a brand owner may want only current, loyal customers with an installed merchant registered app on their mobile device to see certain information about a product to which a tag is attached. Current tag tracking and management systems do not have any mechanism for hiding the functionality of a tag since the tag information is readily discernible to any tag reader application on a mobile device. Conversely a merchant may want to reward customers who use an associated merchant application on a user's device, by granting them access to additional app functionality or content, including product promotional offers, coupons, etc. Typically this requires engaging the customer through a website or other channel to interact with the application. Since it is not always desirable or possible to engage with a customer through such a channel, there is a need in the industry to be able to unlock mobile application features through another technical mechanism.

[0005] This "Discussion of the Background" section is provided for background information only. The statements in this "Discussion of the Background" are not an admission that the any particular subject matter disclosed in this "Discussion of the Background" section constitutes prior art to the present disclosure, and excepting for those portions specifically identified as prior art no part of this "Discussion of the Background" section may be used as an admission that any part of this application, including this "Discussion of the Background" section, constitutes prior art to the present disclosure.

SUMMARY OF THE INVENTION

[0006] Embodiments of the present invention include systems and methods of securing and unlocking functionality of a tag using a mobile application, and, conversely of unlocking functionality of content in a mobile application using a wireless tag.

[0007] One aspect of the disclosure is directed to a computer-implemented method for enabling secure communications between a mobile application executing on a portable computing device and a cloud-based server system, comprising associating a first wireless tag having a first identification code with a tag metadata stored at a cloud based server system; associating the first wireless tag with a secure communications key enabling secure communications between the mobile application and the cloud based server system, where preferably the secure communications key includes at least: a) a first component in the form of a resource locator comprising a first partial portion of the secure communications key, and b) a second component in the form of a payload for the mobile application and comprising a second partial portion of the secure communications key; registering the mobile application with the cloud-based server system; enabling push notifications to the registered mobile application from the cloud-based server system; reading the first wireless tag with the mobile application; communicating a tag payload for the first wireless tag to the cloud based server system; responding to the mobile application by communicating the first partial portion of the secure communications key based on the tag payload through a first network channel; communicating the second partial portion of the secure communications key through a separate second network channel based on confirming that the mobile application is registered for push notifications; and reconstructing the tag metadata after confirming both the first partial portion and the second partial portion of the secure communications key at the mobile applications device. In preferred embodiments, the tag metadata is not included as

part of the first wireless tag, but is useable by the mobile application to provide additional information to a user of the portable computing device about an article to which the first wireless tag is affixed. In other instances, the tag metadata acts as an access key useable by the mobile application to provide functionality to a user of the portable computing device within a restricted area of a mobile application.

[0008] In preferred embodiments, the first wireless tag appears as a conventional tag with a standard payload to mobile applications that are not registered with the cloud-based server system. The only content decodable by a conventional reader is a uniform resource locator (URL). The second partial portion of the secure communications key is preferably dynamically generated and is adapted to expire at an end of a communications session through the separate second network channel. Further in preferred embodiments, the first partial portion of the secure communications key and the second partial portion of the secure communications key are sent in parallel at substantially the same time. In most applications, the first network channel is the Internet, and the second network channel is a message-based network. The first wireless tag is preferably a flexible electronic tag printed with an electronic ink, adapted to respond to a near-field-communications (NFC) interrogation signal, and formatted with non-alterable non-volatile memory data fields identifying at least a manufacturer ID and a product ID.

[0009] Another aspect of the disclosure is directed to a computer-implemented method of enabling enhanced interaction with content associated with a wireless tag on a portable computing device comprising presenting a graphical user interface (GUI) within the portable computing device, which GUI is adapted with a selectable enhanced content option enabling the user to engage with and render enhanced data within the GUI for a physical article associated with the wireless tag; reading a first enhanced experience wireless tag affixed to the physical article with a reader integrated within the portable computing device to determine a first enhanced experience wireless tag identification code; communicating the first enhanced experience wireless tag identification code (TIC) with the portable computing device over a first network to a cloud-based server computing system as part of a request for enhanced experience content (preferably, the request further includes registration data verifying that the portable computing device is registered to receive first enhanced content for the first enhanced wireless tag identification code) receiving a first portion of a communications key for the first enhanced content over the first network at the portable

computing device; receiving a second portion of a communications key for the first enhanced content over a second wireless network at the portable computing device; reconstructing the first enhanced content at the portable computing device using both the first portion of the communications key and the second portion of the communications key; and presenting the first enhanced content on the portable electronic device within the GUI, as part of an enhanced presentation for a physical article (e.g., an item).

[0010] Still another aspect of the disclosure concerns a cloud computing system method for using a wireless tag to present enhanced content for a physical article through a secure channel to a portable computing device comprising: a) associating the first physical article with first enhanced content, where preferably the first enhanced content is configured to be presented within a graphical user interface (GUI) on the portable computing device for the first physical article; b) associating a first enhanced content wireless tag with the first physical article, which first enhanced content wireless tag is coded with a first tag identification code (TIC); c) processing a request from the portable computing device received over a first network for the first enhanced content, the processing including performing a first verification of the TIC presented by the portable computing device within a tag payload, and a second verification of the portable computing device as registered to receive first enhanced content for the first enhanced wireless tag identification code; d) generating and communicating a first partial portion of the first enhanced content to the portable communications device through the first network after the verifications; and e) generating and communicating a second partial portion of the first enhanced content to the portable communications device though a separate second wireless network after the verifications. In this manner, the result is that the first enhanced content is communicated securely and in a form that permits the first enhanced content to be reconstructed by a mobile application and presented on a graphical user interface (GUI) of the portable electronic device. In certain embodiments, a secure communications link is established between the portable computing device and the cloud computing system through a two-factor combination of content communicated through the first network and the second wireless network. The enhanced content for the first enhanced content wireless tag can be presented on a case-by-case basis and only for selected users in selected locations based on the device registration information and user information.

[0011] Other aspects of the disclosure are directed to specialized devices, mobile

computer programs and customized hardware systems that incorporate the above functionalities for creating, presenting and managing enhanced tag experiences which can be enabled from portable devices.

[0012] These and other advantages of the present invention will become readily apparent from the detailed description of various embodiments below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 is a diagram of an exemplary cloud-based tag management system enabling a service provider to, among other functions, coordinate tag creation, tag transfers, tag transactions, tag product assignments, tag marketing, etc. for and between manufacturers, merchants and end users in accordance with the teachings of the present disclosure;

[0014] FIG. 2A is a diagram of an exemplary cloud-based Product Manufacturing/Tag Computing Support system enabling a manufacturer to create and manage tags in connection with product manufacturing operations in accordance with the teachings of the present disclosure;

[0015] FIG. 2B is a diagram of an exemplary cloud-based Tag Mfr/Service Provider Computing Support system enabling a tag service provider to manage and coordinate tags for manufacturers, merchants and end users in accordance with the teachings of the present disclosure;

[0016] FIG. 2C is a diagram of an exemplary cloud-based Merchant Product/Tag Computing Support system enabling a merchant to manage tags, products, etc. in connection with product marketing and sales operations in accordance with the teachings of the present disclosure;

[0017] FIGs. 3A - 3F are diagrams and flowcharts depicting the structure and operation of exemplary tags in accordance with one or more embodiments of the present invention;

[0018] FIG. 4A is a diagram of exemplary hardware and software employed in a mobile computing device implemented as a Tag User Computing Support system enabled with tag management functions in accordance with one or more embodiments of the present invention;

[0019] FIG. 4B depicts an exemplary graphical interface of a mobile computing device enabled with tag management functions in accordance with one or more embodiments

of the present invention;

[0020] FIG. 5A is a diagram of an exemplary cloud-based system enabling an application to unlock enhanced tag data and/or app functions within a mobile computing device for an end user in accordance with the teachings of the present disclosure;

[0021] FIG. 5B depicts an exemplary display on the GUI of a computer or a mobile device presenting an enhanced tag experience for a tagged item in accordance with embodiments of the present invention; and

[0022] FIG. 6 is a flow chart showing an exemplary method for unlocking an enhanced tag data and/or app features experience for a tagged item in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

[0023] Reference will now be made in detail to various embodiments of the invention, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the following preferred embodiments, it will be understood that the descriptions are not intended to limit the invention to these embodiments. On the contrary, the invention is intended to cover alternatives, modifications and equivalents reasonably understood by persons of ordinary skill in the art to be included within the spirit and scope of the invention. Furthermore, in the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be readily apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures and components have not been described in detail so as not to unnecessarily obscure aspects of the present invention. Furthermore, it should be understood that the possible permutations and combinations described herein are not meant to limit the invention. Specifically, it will be understood by those skilled in the art that variations that are not inconsistent may be mixed and matched as desired.

[0024] In the context of this application, some additional guidance is provided for particular terms used herein to better appreciate the scope of the invention. As used herein the term "signal" refers to any known structure, construction, arrangement, technique, method and/or process for physically transferring data or information from one point to another. Unless indicated otherwise from the context of its use herein, the terms

"information" and "data" may be used interchangeably, although each term is generally given its art-recognized meaning. Furthermore, unless indicated otherwise from the context of its use herein, the terms "coupled to," "connected to," and "in communication with" (and grammatical variations thereof) may be used interchangeably and indicate both direct and indirect couplings, connections and communications, but each term is also generally given its art-recognized meaning. Unless indicated otherwise from the context of its use herein, the terms "known," "fixed," "given," "certain" and "predetermined" generally refer to a value, quantity, parameter, constraint, condition, state, process, procedure, method, practice, or combination thereof that is, in theory, variable, but is typically set in advance and not varied thereafter when in use.

[0025] The term "wireless tag" (or simply "tag") as used herein preferably refers to near-field communication (NFC), radio frequency (RF), high frequency (HF), very high frequency (VHF), or ultra high frequency (UHF) tags. The mobile or portable device may comprise a smart phone configured to communicate wirelessly with the wireless tags. The tags may be associated with a user account using a customized tag application on the mobile device.

[0026] In preferred embodiments described herein, the tags are of the NFC type manufactured by Thin Film Electronics ASA (TFEA) in printed integrated circuit (PIC) form (preferably made using TFEA's proprietary printed dopant polysilicon (PDPS) technology) under the tradenames SpeedTap™ and OpenSense.™ In a preferred embodiment, the wireless tags are manufactured using printed doped polysilicon (PDPS) technology (see, e.g., U.S. Pat. Nos. 7,314,513 [Attorney Docket No. IDR0302], 7,485,691 [Attorney Docket No. IDR0422], 8,846,507 [Attorney Docket No. IDR0884], 9,045,653 [Attorney Docket No. IDR1102], and 9,359,513 [Attorney Docket No. IDR1942], the relevant portions of which are incorporated herein by reference).

[0027] A circuit diagram identifying the main components of a preferred example of a tag 300 used in the present embodiments is shown in FIG. 3A. These tags preferably include the following general characteristics:

- Passive (no battery required)
- 13.56MHz operating frequency
- 128 or 256-bit Read-Only Memory (ROM) which is factory programmed and non-electrically modifiable (FIG. 3D).

- 106 Kb/s Data Transfer Rate Manchester bit encoding and OOK load modulation at 847 kHz
- Tag-Talks-First (TTF) Protocol/Mode, meaning the tag preferably transmits its code after it receives enough power from a reader field (FIG. 3E). The tag does not wait for or require any additional commands from a reader before transmitting its code, and for security reasons, preferably does not acknowledge/recognize any commands from the reader
- Adheres to Subset of ISO14443A
- 16 bits CRC for data integrity verification
- Operating Range of a Few Centimeters to enable Tap event detection (depends on field strength, antenna design, etc.)
- Single-tag mode for precise one-on-one interaction

[0028] Additional details may be found in datasheets published by TFEA for its tag products, including in materials identified as Thinfilm NFC Barcode Protocol for NFC OpenSense™ & NFC SpeedTap™ Tags available at the manufacturer's website as of the date of filing of this application and incorporated by reference herein.

[0029] As seen in FIGs. 3B, 3C and 3E, these types of tags preferably comply with the NFC Barcode protocol, a common NFC protocol supported by top-tier NFC controllers from NXP, Broadcom, Samsung, Sony, Toshiba, and others. The tags are preferably passive, 128-bit NFC tags operating at 13.56MHz and using a Tag-Talks-First (TTF) protocol. These types of NFC tags operate preferably in a read-only mode to transmit 128-bit codes to NFC-enabled devices, such as phones, tablets, PCs, and set-top boxes. Preferably the data in the tags is also primarily stored in permanent, unalterable read-only memory but may in some embodiments include a number of reprogrammable dynamic bits to reflect the status of connected or integrated sensors and other information that could change over time. Because these types of tags do not receive information via RF, all data transmissions are unidirectional, from tag 300 to reader 310.

[0030] The NFC SpeedTap and NFC OpenSense tags also preferably store data following the NFC Barcode data formats (previously known as the Kovio NFC Barcode data formats). These are standardized representations of data so that operating systems and applications can consistently interpret the 128-bit data stream. An example of a memory map

330 preferably used by such tags is shown in FIG. 3D. As seen in FIG. 3D the tags preferably include dedicated fields for such parameters as a manufacturers ID field 332, a data format specifier field 334, a data payload field 336 and a CRC field 338.

[0031] In a preferred embodiment the 128 bit code 330 includes an 8-bit (1-byte) Manufacturer ID field 332 consisting of a start bit and a 7-bit ID. Under current standards, when implementing a Tag-Talks-First (TTF) format of an NFC Barcode, it is typically required that the first bit is set to '1' to serve as an identifiable start bit for an NFC controller that is attempting to read the tag. A 7-bit manufacturer ID (based on the least significant 7 bits of the manufacturer IDs specified in the ISO/IEC 7816-6 specification) follows the standard logical '1' start bit. An 8-bit (1-byte) data format identifier field 334 then describes how an NFC reader should interpret the contents of the payload field 336. The data format identifier preferably contains two sections: Reserved bits and a Data Type Format. In one preferred embodiment the 3-bit Reserved section is set to '000' for a 128-bit NFC Barcode. A 5-bit Data Type Format allows for 32 possible data types. The data payload field 336 is preferably 96 bits, and may include separate components, such as a tag ID 336a, an object/item ID 336b and a vendor ID 336c or some other convenient format for the application in question. The payload 336 can be used for any number of data purposes including for identifying a uniform resource locator (URL) having different formats, an electronic product code (EPC) or any other desired identification/metadata information. The CRC field 338 can be coded in accordance with any number of conventional specifications as needed to support a particular application. In preferred embodiments described herein the tag identification codes are assigned to products in accordance with the teachings of application serial no. 15/904,178 also assigned to the present applicant, and hereby incorporated by reference. Again, it should be understood that other NFC Barcode data formats can be used in other applications, and as standards for tags evolve, it is expected that other variations will be employed in the future.

[0032] As seen in FIGs. 3B and 3C, when placed proximate to such that it can communicate with an NFC compatible reader 310 (see FIG. 3B) the tag (initially in a sleep mode) transmits after a wake-up time (typically 5ms) in the presence of a sufficiently large interrogation field. As used herein, a "tap" or "tapping event" refers to the transmission of the NFC code by the tag when it is sufficiently close to be read by an NFC controller as may be embodied in a portable computing device (e.g. smartphone). Those skilled in the art will

appreciate that the term "tap" in this instance does not require physical contact or bumping of the tag, but, rather, merely waving or placing the reader in close proximity to the tag. The distance range of detectable taps or tapping events can be adjusted of course, by altering field strength, reader antenna size and other physical/transmission parameters. As seen in FIGs. 3C and 3E, the tag continues, at a predetermined interval and standardized protocol, to re-transmit the entire length as long as the NFC Barcode is powered up in the reader's field. The transmission intervals are separated by sleep cycles, which timing periods are again predefined according to an operating standard used in the particular application.

[0033] In addition to other applications, wireless near field communication (NFC) and radio frequency (RF) security and/or identification tags can be used by manufacturers, distributors and other entities to digitally identify, track and manage products and other objects. The term "owned" in connection with a tag means generally that it is associated with a user account by the manufacturer of the tags before receipt by the user (e.g., a product manufacturer, distributor, reseller, packager, end user [consumer], etc.). The term "give-away" refers to tags are not pre-associated with a user account, and may be associated with a user account by the user of the mobile device. Give-away tags may be given away at conferences or demonstrations or as samples, or may be sold as a commodity item.

[0034] The term "group" when used herein preferably refers to tags manufactured on a common roll or sheet, and/or which have at least some common manufacturing ID 332 (FIG. 3D) data, payload data 336, etc. It will be understood that in some embodiments, tags which have different physical tag ids 330 may nonetheless be logically associated to create groupings at different logical levels by the support software described herein.

[0035] Note that in the present disclosure, like numbered structures/steps in the drawings are intended to reference the same or substantially the same structure/step in counterpart drawings.

Tag Management System Architecture

[0036] FIG. 1 is a diagram of an exemplary cloud-based tag management system 100 enabling a service provider to, among other functions, coordinate tag creation, tag transfers, tag transactions, tag product assignments, tag marketing, etc. for and between manufacturers, merchants and end users in accordance with the teachings of the present disclosure. The tag management system 100 preferably includes a front-end cloud computer system 110 and a back-end cloud computing system 170 connected through a secure connection 114. The

system 100 further preferably includes separate computing support systems for the different tag stakeholders, including a Product Manufacturing/Tag Computing Support system 140 (shown in more detail in FIG.2A) a Tag Mfr/Service Provider Computing Support system150 (shown in more detail in FIG. 2B) and a Merchant Product/Tag Computing Support system 160 (shown in more detail in FIG. 2C), all of which preferably include respective suitable portal application software to permit interfacing with their corresponding cloud support systems. It will be understood by those skilled in the art that the functionalities of each of these separate systems may be subsumed and/or integrated into the cloud environments 110/170 respectively in different applications. The tag management system further preferably comprises a tag user computing support system for end-users, including consumers, including one or more mobile devices 120 (or conventional PCs) executing a mobile tag manager application 125 (or web portal 126) and connected through both TCP/IP protocol network 105a (preferably the Internet) and a cellular network 105b. Various forms of tags can be managed by system 100 including wireless security tags (e.g., continuity sensing tag 135') a wireless identification tag 135, and other known types.

[0037] The cloud computing systems (110, 170) may provide shared computer processing resources and data to the other devices in the system, and may be implemented using a cloud computing service such as Google Cloud Platform™ or Amazon Web Services™. The computing systems (110, 170) may be implemented using a service model such as software as a service (SaaS). Some or all of the data may be accessed by authorized users, but is protected from access by unauthorized users.

[0038] In the SaaS service model, the tag manufacturer (service provider) applications (e.g., the mobile application 125 or portal application 126) may be partially executed using the cloud computer 110. The tag manufacturer applications are accessible from a support system 150, as well as through various client devices (such as the mobile device 120) through either a web browser or a program (e.g., application) interface. In a preferred embodiment the various stakeholders, including tag manufacturer, product manufacturers, merchants (distributor, reseller) or end-users do not manage or control the underlying infrastructure in the cloud computer 110 or 170 including any network, servers, operating systems, and/or storage devices. As will be apparent to skilled artisans, FIG. 1 depicts only those components of system 100 critical to understanding the present teachings. Moreover, other components and software modules may be employed in system 100

consistent with the present teachings.

[0039] FIG. 2A is a diagram of an exemplary cloud-based tag manufacturing support system enabling a manufacturer to create and manage tags with a back end cloud computing system for product manufacturing operations in accordance with the teachings of the present disclosure. System 170 is a back end cloud computing system that includes one or more computing servers 172, product database 178, tag database 179 and related software modules that support manufacturers integrating tags with any type of product/object, such as apparel, consumables, household items, pharmaceuticals, or any other commercial article 137 on which a tag 135 or 135' (which can be in the form of a roll, sheet, etc.) can be affixed directly or as part of packaging during a manufacturing process. The product-tag support system further preferably comprises a host computing system 140 (e.g. a PC, smartphone, etc.), typically onsite at the product manufacturer facility, which system further includes a portal application (not shown, but which may take on any number of conventional forms) to permit communications with a cloud system 170, including a manufacturing administrative module 174, a manufacturing interface module 173, and various tag ID management applications in module 177. A manufacturer tag writer/application module 176 controls the application of tags to products/packaging during the manufacture of the articles of interest at a fabrication facility 175. The various software modules of FIG. 2A assist product manufacturers in managing the creation, application and tracking of products including tags.

[0040] A manufacturing admin module 174 provides visualization and configuration tools, including for enabling users to designate particular tag types/IDs for particular products. The tag IDs are provided by a tag manufacturer through an interface module 173 by a service provider, or, in some instances can be generated directly by a tag ID management module 177. Under either scenario, a product manufacturer can maintain separate databases of both tags (M-Tag 178) and products (M-Product 179). The type and form of the data in such databases may be specified in any convenient form most suitable for the manufacturer's particular operations, infrastructure, etc. Since it is conceivable that the same tag or product can be managed and tracked differently by different stakeholders using different data formats and logical identifiers, the nomenclature in FIG. 2A, i.e., M-Prod db 179 and M-Tag dB 178 denotes such distinction. The application of specific tag ids to specific products is controlled and monitored by a module 176 at the product manufacturing facility 175. In this manner, a product manufacturer can maintain an accurate inventory and

record of tag/product pairings. This product/tag pairing data 176' then be shared with other systems as desired, including through an API call or other known mechanisms known in the art. While shown as part of front end cloud computing system 170, it will be appreciated by those skilled in the art that some or all portions of such modules, databases, interfaces, etc. in FIG. 2A can be implemented as part of host computing system 140 as well.

[0041] FIG. 2B is a diagram of an exemplary cloud-based tag service provider support system enabling a tag service provider to create, manage and coordinate tags for manufacturers, merchants and end users in accordance with the teachings of the present disclosure. A front end cloud-computing system 110 is accessed by a tag manufacturing (and/or tag service provider) host system 150. As seen in FIG. 2A, tags 135 are manufactured in a tag fabrication facility 138 in the form of rolls, sheets, or other conventional forms. The tags are physically coded during manufacture in accordance with any number of tag identification code types and formats (see e.g. FIG. 3, 336a, 336b, 336c). System 110 includes specified by a tag management module 156, which is a front end cloud computing system that includes one or more computing servers 112, a tag ID (S-tag) database 158, a tag metadata database 159, a user identification code database 157, and related software modules that support tag creation support and management functions. The type and form of the data in such databases may be specified in any convenient form most suitable for the tag provider's particular operations, infrastructure, etc. As the tag IDs tracked by system 110 may be the same or have different physical IDs than those tracked by system 170, the tag IDs are designated with a (potentially) different dB index (i.e., S-tag as opposed to M-tag).

[0042] The tag manufacturer/provider system further preferably comprises a host computing system 150 (e.g. a PC, smartphone, etc.), typically onsite at the tag manufacturer facility, which system further includes a portal application (not shown, but which may take on any number of conventional forms) to permit communications with a cloud system 110, including a service administrative module 154, a manufacturing interface module 152 which communicates over a secure connection to back-end cloud system 170 and to a merchant support system 160 (FIG. 2C) and a tag management module 156 that comprises various tag ID management applications. A tag engagement module 151 interacts with and coordinates transactions with end-user systems, as seen in FIG. 2D, including through receipt and processing of tap events, user identification information, and related context data from user computing devices. Tag engagement module 151 further generates and provides any

necessary responses from system 110 as described further below, including tag AR metadata, enhanced tag secure data, tag ownership transaction details and tag identification codes. The various software modules of FIG. 2D assist product manufacturers in managing the creation, application and tracking of products including tags. While shown as part of front end cloud computing system 110, it will be appreciated by those skilled in the art that some or all portions of such modules, databases, interfaces, etc. in FIG. 2B can be implemented as part of host computing system 150 as well.

[0043] FIG. 2C is a diagram of an exemplary cloud-based tag merchant support system enabling a merchant to manage tags, products, etc. in connection with product marketing and sales operations in accordance with the teachings of the present disclosure. A front end cloud-computing system 110 is accessible to a merchant product/tag host system 160. As seen in FIG. 2C, product/tag ID information 176' from one or more manufacturers can be input from a source including a back-end cloud computing system 170 (FIG. 2A). In the example shown in FIG. 2C, the product is a consumable item (beer) 137, which has an affixed tag (integrated as part of the label). A merchant/vendor can customize additional content for the product, including multi-media data (video, audio, graphics, etc.) 138 which can be presented when the product tag is read as part of an augmented reality (AR) experience discussed further below.

[0044] System 160 includes a combination of hardware and software components that support merchant (retailer/distributor) product-tag marketing, promotions and sales operations, including one or more server computing machines 164, a host computing system 161, and associated databases containing content and index data for tags (R-Tag db 163), products (R-Product db 169), customers (R-Customer db 167) and customized content (R-Custom Content db 167). The type and form of the data in such databases for such entities may be specified in any convenient form most suitable for the merchant's particular operations, infrastructure, etc. System 160 also supports a merchant website 139, which can be configured with product/marketing/sales webpages in any number of styles known in the art and made accessible to web-enabled browsers (including on smartphones) through conventional uniform resource locators (URLs). Resources and control access to system 160 can also be made through secure applications executing on smartphones 161' and similar portable computing devices.

[0045] The tag manufacturer/provider system further preferably comprises a host

computing system 161 (e.g. a PC, smartphone, etc.), typically onsite at the merchant facility, which system further includes a portal application (not shown, but which may take on any number of conventional forms) to permit communications with a cloud system 110. Merchant support system 160 further includes a number of software modules, including a merchant (retailer/distributor or R-tag) management module 165 that enables and supports tag creation, tag-product association, tag-content association, and related management/marketing functions attendant to the marketing, promotion and sales of products including physical tags. As the tag IDs tracked by system 160 may be the same or have different physical IDs than those tracked by systems 110/170, the tag IDs are designated with a (potentially) different dB index (i.e., R-Tag, as opposed to S-tag and/or M-tag).

[0046] System 160 may further include an AR Context Rules module 163 and AR Device Rendering Logic module 166, which are responsible for identifying, selecting and presenting customized content to end-user devices 120 within a customized application 125 (see FIG. 1) or as part of a customized experience within a browser accessing website 139. In general, AR Context Rules module 163 dictates user, time, place, manner controls and filters, so that, for example, certain content may be presented for a designated product tag ID (i.e. wool sweater) only to selected users meeting certain criteria (i.e. new customers) at particular locations (i.e., designated partner store) at particular times (i.e. in fall months). All of such parameters can be extracted from the end-user's device 121, product tag 135 and other merchant customer information in db 167. Other examples of context controls will be apparent to those skilled in the art, and may be selected/customized on a tag-by-tag, or customer-to-customer basis. Providing similar support is AR Device Rendering Logic module 166, which is responsible for providing appropriate metadata in the right format for the particular desired AR experience on a target device. For example, a merchant may specify that a designated graphics overlay with particular dimensions should be made on a particular portion of a target device (i.e., model A smartphone by brand X). Again, any form of software tools and controls for overlaying, supplementing and augmenting existing media files (e.g., a graphical image captured by a phone) can be used for this module. While shown as a standalone system in FIG. 2C, it will be understood by skilled artisans that part or all of system 160 could be implemented by front end cloud computing system 110 and controlled/managed through portal applications with basic devices 161, 161' and the like.

[0047] FIG. 4A is a diagram of exemplary hardware and software employed in a

mobile computing device 120 enabled with tag management functions in accordance with one or more embodiments of the present invention. The device 120 includes a customized CPU 122 for executing mobile applications, a memory 123 (which may take different forms, including volatile DRAM/SRAM and non-volatile EEPROM), a set of different types of sensors 124 (camera, microphone, touch, gyroscopic to name a few) for capturing different physical stimuli, a Universal Integrated Circuit Card (UICC) or SIM card 126 for communicating over a cellular channel (such as a carrier network 105), Bluetooth/GPS and WiFi communication circuits 127, and various I/O circuits, including display, speakers, etc. Most usefully, as concerns the present disclosure, a mobile computing device includes one or more Near Field Communication (NFC) support circuits, including an NFC communications IC 121a, an associated Secure Element 121b and an NFC receive/transmit antenna 121c. Device 120 further includes a number of firmware and software components, including an Operating System (OS) 125a (e.g., Android, IOS), a web/network software interface 125b (e.g., Safari, Chrome, etc.) for establishing communication sessions over an IP network channel 105a (e.g. Internet) and one or more software applications 125c executing on the device and enabling different functions I/O and computational functions.

[0048] For purposes of the present disclosure, user applications which are of most interest are shown in FIG. 4B which depicts an exemplary graphical interface of a mobile computing device enabled with tag management functions in accordance with one or more embodiments of the present invention. These applications generally include an augmented reality (AR) tagged Item application 129a, an enhanced tag/app application 129b, a tag transfer application 129c, an assign new tag application 129d, and a provisions tag application 129e. It will be understood by skilled artisans that other hardware and software components may be included in embodiments of a mobile computing device 120 discussed herein.

Enhanced Tag/Application

[0049] In some commercial applications it may be desirable to obscure or quasi-encrypt portions of the payload of a tag, or conversely, to enhance the payload in accordance with merchant rule sets or context to tailor an end user experience. For example, a tag A affixed to an article of clothing B may have a payload C that is readable by a generic reader application, and includes a simple URL D to a merchant site E that includes basic product marketing information F about the item. The end user in this instance is thus provided a

basic level or experience F from tag A. In embodiments of the present disclosure, a registered enhanced tag application on the user's device is configured to read the same tag A, and render additional information G (including promotional or marketing information) securely to an end-user from a tag service provider computing system complementing the merchant's native computing operations. For example, a merchant may want known existing customers to obtain additional promotional discounts when sampling products when they visit particular establishments at particular times. In other instances a merchant may want to engage in a secure, two-factor authentication transaction with the end user. These experiences can be controlled using the dynamic tag provisioning system disclosed herein. Conversely a merchant may want to encourage potential customers to use an associated merchant application on a user's device. This functionality can be enabled by encouraging potential customers to interact with tags as a condition of unlocking additional enhanced application functions.

[0050] FIGs. 5A - 5B are diagrams of an exemplary cloud-based system 1600 enabling an application to unlock secured enhanced tag data and/or app functions respectively within a mobile computing device for an end user in accordance with the teachings of the present disclosure. In FIG. 5A an enhanced, secure tag experience is enabled by merchant related components in the front-end cloud computing system 110 that cooperate with requests from an application 522 executing on user devices 520. As seen in FIG. 5A an article of clothing 533 includes an associated tag 535. Each tag includes a unique ID as explained above. An application 522 on device 520 is activated and used to read the tag 535 using NFC with a tap gesture as further noted above. After reading the tag information 826d, the application 522 invokes an enhanced tag experience for the object, and then preferably communicates the details of the tap event 826a, including the tag payload (which may include a tag ID as well, along with object ID data) along with user identification (UID), app registration information and location information to tag engagement module 151 (FIG. 2B) in front-end cloud computing system 110 over network channel 105a. In response to such enhanced tag request, a first partial payload for the tag 826b is retrieved from db 159 (FIG. 2B) and returned to device 520 through IP channel 105a where it can be rendered on the user's device in accordance with parameters provided by a merchant computing system 160 (FIG. 2C) including context rules 163 and rendering logic 166. In a first basic embodiment, the 1st partial payload is simply a URL, and communicates nothing more than this basic

information, which can be presented within a browser or app portion 527 of display 525. Notably, this 1st partial payload can also be derived from the tag payload but non-registered applications, but it does not provide any inkling or hint of additional functionality bound up in the tag. The cloud computing system 110 then verifies if the application 522 is registered for push notifications, checks the tag ID to determine if it is valid as well, and, if so, pushes an additional 2nd portion of the tag payload 826c (which is preferably encrypted and generated dynamically) to device 520 over a second, separate channel 105b. Application 522 then decrypts the second payload, and combines the two payloads to reconstruct an enhanced payload for the tag. This then permits additional functionality for the tag, which may include, for example, additional content or URLs that identify hidden information and offers for other products that are presented in another portion 528 of display 525. Other examples of enhanced tag functionality provisioning will be apparent to skilled artisans. The 2nd payload and enhanced payload have a limited lifetime, and are treated as valid by cloud computing system 110 only during a single session. The combination of two separate components, including the first partial payload and the second partial payload, constitute effectively a form of secure communications key between the user's device 520 and cloud computing system 110.

[0051] Referring to FIG. 5A again, in the example shown, a webpage 527 for the tagged product is presented and supplemented with enhanced metadata 528 (in this instance, information on offers of related products) generated from reconstructing an enhanced tag payload from the two partial payloads received from different channels. As noted above, to further secure the tag functionality, the second portion of the payload is dynamic and only valid during the duration of the user's session. In essence, the embodiment of FIG. 5A permits a form of secure messaging between the cloud computing system 110 and the user device 520, which is enabled through selected tags. Those skilled in the art will appreciate that other components can be utilized in system 500 in accordance with the present teachings.

[0052] FIG. 5B shows a similar complementary use of system 500 in which an enhanced, secure application experience is enabled by NFC tags that unlock additional functionality in a user device. For example, it is possible to secure sections of a mobile application, and make them accessible only by unlocking them with a designated key. As seen in FIG. 5B an item 533 (in this case, a bottle of beer) includes an associated tag 535. Each tag includes a unique ID as explained above. An application 522 on device 520 is

activated and used to read the tag 535 using NFC with a tap gesture as further noted above. After reading the tag information 826d, the application 522 invokes an enhanced application experience for the object, and then preferably communicates the details of the tap event 526a, including the tag payload (which may include a tag ID as well, along with object ID data) along with user identification (UID), app registration information and location information to tag engagement module 151 (FIG. 2B) in front-end cloud computing system 110 over network channel 105a. In response to such enhanced application request, a first partial payload for the tag 526b is retrieved from db 159 (FIG. 2B) and returned to device 520 through IP channel 105a where it can be rendered on the user's device in accordance with parameters provided by a merchant computing system 160 (FIG. 2C) including context rules 163 and rendering logic 166. In a first basic embodiment, the 1st partial payload is simply a URL, and communicates nothing more than this basic information, which can be presented within a browser or app portion 527 of display 525. Notably, this 1st partial payload can also be derived from the tag payload by non-registered applications, but it does not provide any inkling or hint of additional functionality bound up in the tag. The cloud computing system 110 then verifies if the application 522 is registered for push notifications, checks the tag ID to determine if it is valid as well, and, if so, pushes an additional 2nd portion of the tag payload 526c (which is preferably generated dynamically and encrypted) to device 520 over a second, separate channel 105b. Application 522 then decrypts the second component, and combines the two payloads to reconstruct an enhanced payload for the tag. This then permits additional functionality (unlocks features) for application 522, which may include, for example, additional content or URLs that identify hidden information and offers for other products that are presented in another portion 528 of display 525. Other examples of enhanced application functionality provisioning will be apparent to skilled artisans. The 2d payload and enhanced payload have a limited lifetime, and are treated as valid by cloud computing system 110 only during a single session. As before, the combination of two separate components, including the first partial payload and the second partial payload, constitute effectively a form of secure communications key between the user's device 520 and cloud computing system 110.

[0053] Referring to FIG. 5B again, in the example shown, a webpage 527 for the tagged product is presented and supplemented with enhanced metadata 528 (in this instance a coupon for the user for the beer product) generated from reconstructing an enhanced tag

payload from the two partial payloads received from different channels. Similar benefits, such as loyalty points, or access to premium services may also be offered or included as part of the enhanced tag payload. As noted above, to further secure the tag functionality, the second portion of the payload is preferably encrypted, dynamic and only valid during the duration of the user's session. Persons skilled in the art will appreciate that other functions can be unlocked on a user's device, or through applications on the user's device, based on the two-factor process described, in which different components of a tag payload are combined to unlock part of an application for a limited authenticated session process.

[0054] FIG. 6 is a flow chart showing an exemplary method 600 for unlocking an enhanced tag data and/or app features experience for a tagged item in accordance with embodiments of the present invention. At step 602, a user may elect to have his/her tag app and/or device registered at cloud system 110. At step 605, a user tap on a tag for an article is detected by device 520 in the manner described above in connection with FIGs. 3A-3F. The tag id (included in some or all of payload 136) is then extracted and read at step 610. The user id (which may be any one or more of a username, password, or application registration ID) and location data can also be derived from the application and device sensors (i.e. GPS and similar techniques) at step 615. A formal user enhanced tag request is then presented to cloud computing system 110 at step 620, which then determines at step 630, from available tag and uid databases (FIG. 2B, databases 157/158) if the request is valid. When these request parameters are invalid, the process simply terminates at step 625, by returning a reply to the user that there is no available data for the tag in question. When the Tag and UID information (which may include a device or application ID) are determined to be valid, a 1st portion of the tag payload is returned through an IP based channel 105a back to the user's device. As seen in FIG. 5A, this first component of the tag payload may be simply a URL to a merchant or tag service provider webpage with base product information. As with prior embodiments, context and rendering rules (FIG. 2C, modules 163/166) may be considered and processed as well for determining applicability of the 1st tag payload to the particular user, device, time, location, etc. At step 640, cloud computing system 110 determines if the user's application and/or device is/are registered for push notifications. When the registration determination is negative, no further payload or tag information is presented to the user device and, at least for the tag in question, the session is deemed completed at step 645. At step 650, when the user application/device is/are registered, the second portion or component of the tag payload

(which may or may not be encrypted) is returned to the user's device 620 through a separate network channel, which may be a cellular network. The total tag payload based on the two separate payload components is then reconstructed at the user's device in accordance with any number of known techniques at step 655. For example, the second component of the tag may be encrypted according to a known encryption process, such that it can be decrypted with a private key on application 623. At step 660, when the tag functionality is unlocked from the two-stage authentication process, additional metadata or content can be presented within the application, as seen in FIG. 5A.

[0055] Conversely, in the case of unlocking additional application functionality, the process flow proceeds to step 665, as seen in FIG. 5B. The reconstructed app payload is used as a form of key to unlock any secured areas of application 622 controlled by a particular merchant/vendor associated with the tag 635 in question.

[0056] This form of engagement with end-users described above permits customization and enhancement of tags without requiring dedicated, fixed tag identification codes provided at a factory. Instead, tag functionality can be enhanced through a secure exchange by a mobile application with a cloud computing server. Similarly, content and functions of a mobile application can be unlocked through physical tags, and without requiring further engagement with the end-user with a merchant website or the like.

[0057] It will be understood by those skilled in the art that the above descriptions are merely examples and that countless variations of the same can be implemented in accordance with the present teachings. A number of other conventional steps that would be included in a commercial application have been omitted, as well, to better emphasize the present teachings.

[0058] It will also be apparent to those skilled in the art that the modules of the present invention, including those illustrated in the figures can be implemented using any one of many known programming languages suitable for creating applications that can run on large scale computing systems, including servers connected to a network (such as the Internet) as part of a cloud computing system. The details of the specific implementation of the present invention will vary depending on the programming language(s) used to embody the above principles, and are not material to an understanding of the present invention. Furthermore, in some instances, a portion of the hardware and software will be contained locally to a user's computing system, which can include a portable machine or a computing machine at the user's premises, such as a personal computer, a PDA, digital video recorder,

receiver, etc.

[0059] Furthermore, it will be apparent to those skilled in the art that this is not the entire set of software modules that can be used, or an exhaustive list of all operations executed by such modules. It is expected, in fact, that other features will be added by system operators in accordance with customer preferences and/or system performance requirements. Furthermore, while not explicitly shown or described herein, the details of the various software routines, executable code, etc., required to effectuate the functionality discussed above in such modules are not material to the present invention, and may be implemented in any number of ways known to those skilled in the art. Such code, routines, etc. may be stored in any number of forms of machine readable media. It is understood that the protection afforded the present invention also comprehends and extends to embodiments different from those above, but which fall within the scope of the claims presented below.

CLAIMS

What is claimed is:

1. A computer-implemented method for enabling secure communications between a mobile application executing on a portable computing device and a cloud-based server system, the method comprising:

associating a first wireless tag having a first identification code with a tag metadata stored at a cloud based server system;

associating said first wireless tag with a secure communications key enabling secure communications between the mobile application and the cloud based server system, said secure communications key including at least:

a) a first component in the form of a resource locator comprising a first partial portion of said secure communications key;

b) a second component in the form of a payload for the mobile application and comprising a second partial portion of said secure communications key;

registering the mobile application with the cloud-based server system;

enabling push notifications to the registered mobile application from the cloud-based server system;

reading said first wireless tag with the mobile application, and communicating a tag payload for said first wireless tag to the cloud based server system;

responding to said mobile application by communicating said first partial portion of said secure communications key based on said tag payload through a first network channel;

communicating said second partial portion of said secure communications key through a separate second network channel based on confirming that said mobile application is registered for push notifications; and

reconstructing said tag metadata after confirming both said first partial portion and said second partial portion of said secure communications key at the mobile applications device, wherein the tag metadata is not included as part of the first wireless tag but is useable by the mobile application to provide additional information to a user of the portable computing device about an article to which the first wireless tag is affixed.

2. The method of claim 1, wherein said first wireless tag appears or is read as a conventional tag with a standard payload to mobile applications that are not registered with the cloud-based server system.

3. The method of claim 1, wherein said first partial portion of said secure communications key is a uniform resource locator (URL).

4. The method of claim 1, wherein said second partial portion of said secure communications key is dynamically generated and is adapted to expire at an end of a communications session through said separate second network channel.

5. The method of claim 1, wherein said first partial portion of said secure communications key and said second partial portion of said secure communications key are sent in parallel at substantially the same time.

6. The method of claim 1, wherein said first network channel is the Internet, and said second network channel is a message-based network.

7. The method of claim 1, wherein said first wireless tag is formatted with non-alterable non-volatile memory data fields identifying at least a manufacturer ID and a product ID.

8. The method of claim 1, wherein said first augmented experience wireless tag comprises a flexible electronic tag printed with an electronic ink.

9. The method of claim 1, wherein said first augmented experience wireless tag is adapted to respond to a near-field-communications (NFC) interrogation signal.

10. The method of claim 1, wherein the first augmented experience wireless tag is configured in a continuous, low power transmit mode.

11. A computer-implemented method for enabling secure communications between a mobile application executing on a portable computing device and a cloud-based server system, the method comprising:

specifying a first wireless tag as an access key for a restricted area accessible within the mobile application;

associating said first wireless tag with a secure communications key enabling secure communications between the mobile application and the cloud based server system, said secure communications key including at least:

a) a first component in the form of a resource locator comprising a first partial portion of said secure communications key;

b) a second component in the form of a payload for the mobile application and comprising a second partial portion of said secure communications key;

registering the mobile application with the cloud-based server system;

enabling push notifications to the registered mobile application from the cloud-based server system;

reading said first wireless tag with the mobile application in response to a tap event generated based on the portable communications device contacting said first wireless tag;

communicating a tag payload for said first wireless tag to the cloud based server system based on or in response to confirming said tap event;

responding to said mobile application by communicating said first partial portion of said secure communications key based on said tag payload through a first network channel;

communicating said second partial portion of said secure communications key through a separate second network channel based on confirming that said mobile application is registered for push notifications; and

reconstructing said access key after confirming both said first partial portion and said second partial portion of said secure communications key at the mobile applications device, wherein the access key is not included as part of the first wireless tag but is useable by the mobile application to provide functionality to a user of the portable computing device within said restricted area of the mobile application.

12. A computer-implemented method of enabling enhanced interaction with content associated with a wireless tag on a portable computing device, the method comprising:

presenting a graphical user interface (GUI) within the portable computing device, wherein the GUI is adapted with a selectable enhanced content option enabling the user to engage with and render enhanced data within the GUI for a physical article associated with the wireless tag;

reading a first enhanced experience wireless tag affixed to the physical article with a reader integrated within the portable computing device to determine a first enhanced experience wireless tag identification code;

communicating said first enhanced experience wireless tag identification code (TIC) with the portable computing device over a first network to a cloud-based server computing system as part of a request for enhanced experience content;

wherein said request further includes registration data verifying that the portable computing device is registered to receive first enhanced content for said first enhanced wireless tag identification code;

receiving a first portion of a communications key for said first enhanced content over said first network at the portable computing device;

receiving a second portion of a communications key for said first enhanced content over a second wireless network at the portable computing device;

reconstructing said first enhanced content at the portable computing device using both said first portion of said communications key and said second portion of said communications key; and

presenting said first enhanced content on the portable electronic device within the GUI as part of an enhanced presentation for the physical article.

13. The method of claim 12, wherein said first enhanced experience wireless tag identification code includes a uniform resource locator (URL) but no other enhanced content for the physical article.

14. The method of claim 12, further comprising establishing a secure communications link between the portable computing device and said cloud computing system through a two-factor combination of content communicated through said first network and said second wireless network.

15. The method of claim 14, wherein said secure communications link has a limited temporal duration and extends only for a current session between the portable computing device and said cloud computing system.

16. The method of claim 12, further comprising registering a mobile application executing on the portable computing device with said cloud computing system for push notifications for said first enhanced content.

17. The method of claim 12, further comprising unlocking one of a function or feature of a mobile application executing on the portable computing device in response to reconstructing said first enhanced content.

18. The method of claim 12, wherein said first partial portion of said secure communications key and said second partial portion of said secure communications key are received at substantially the same time.

19. The method of claim 12, wherein said first enhanced wireless tag comprises a flexible electronic tag printed with an electronic ink.

20. The method of claim 12, wherein said first enhanced wireless tag is adapted to respond to a near-field-communications (NFC) interrogation signal.

21. A computer-implemented method for using a wireless tag to present enhanced content for a physical article through a secure channel to a portable computing device using a cloud computing system, the method comprising:

a) associating a first physical article with first enhanced content, wherein the first enhanced content is configured to be presented within a graphical user interface (GUI) on the portable computing device for the first physical article;

b) associating a first enhanced content wireless tag with the first physical article, which first enhanced content wireless tag is coded with a first tag identification code (TIC);

c) processing a request from the portable computing device received over a first network for said first enhanced content, said processing including performing a first verification of said TIC presented by the portable computing device within a tag payload, and a second verification of the portable computing device as registered to receive first enhanced content for said first enhanced wireless tag identification code;

d) generating and communicating a first partial portion of said first enhanced content to the portable communications device through the first network after verifications; and

e) generating and communicating a second partial portion of said first enhanced content to the portable communications device though a separate second wireless network after verifications, wherein said first enhanced content is communicated securely and in a form that permits said first enhanced content to be reconstructed by a mobile application and presented on a graphical user interface (GUI) of the portable electronic device.

22. The method of claim 12, wherein said first partial portion of said first enhanced content includes a uniform resource locator (URL) but no other enhanced content for the physical article.

23. The method of claim 21, further comprising establishing a secure communications link between the portable computing device and said cloud computing system through a two-factor combination of content communicated through said first network and said second wireless network.

24. The method of claim 23, wherein said second partial portion of said first enhanced content is dynamically generated and configured with a limited temporal duration.

25. The method of claim 21, further comprising registering a mobile application executing on the portable computing device with said cloud computing system for push notifications for said first enhanced content.

26. The method of claim 21, wherein said first enhanced content enables unlocking one of a function or feature of a mobile application executing on the portable computing device.

27. The method of claim 21, wherein said first enhanced content enables a user of the portable computing device to receive an electronic coupon from a merchant without requiring access to said merchant's website or other electronic storefront.

28. The method of claim 21, wherein said first partial portion of said secure communications key and said second partial portion of said secure communications key are communicated at substantially the same time.

29. The method of claim 21, wherein said enhanced content for said first enhanced content wireless tag is presented on a case-by-case basis and only for selected users in selected locations.

30. The method of claim 21, wherein said enhanced content includes promotional discounts for said first physical article.

31. A computing system configured to enable secure communications between a mobile application executing on a portable computing device and a cloud-based server system comprising:

one or more software modules adapted to execute on the portable computing device and/or the cloud-based server system and perform at least the following functions:

associate a first wireless tag having a first identification code with tag metadata stored at a cloud based server system;

associate said first wireless tag with a secure communications key enabling secure communications between the mobile application and the cloud based server system, said secure communications key including at least:

a) a first component in the form of a resource locator comprising a first partial portion of said secure communications key; and

b) a second component in the form of a payload for the mobile application and comprising a second partial portion of said secure communications key;

register the mobile application with the cloud-based server system;

enable push notifications to the mobile application from the cloud-based server system based on said registering;

read said first wireless tag with the mobile application, and communicate a tag payload for said first wireless tag to the cloud based server system;

respond to said mobile application by communicating said first partial portion of said secure communications key based on said tag payload through a first network channel;

communicate said second partial portion of said secure communications key through a separate second network channel based on confirming that said mobile application is registered for push notifications; and

reconstruct said tag metadata after confirming both said first partial portion and said second partial portion of said secure communications key at the mobile applications device, wherein the tag metadata is not included as part of the first wireless tag but is useable by the mobile application to provide additional information to a user of the portable computing device about an article to which the first wireless tag is affixed.

32. A computer program having executable instructions stored on a non-transitory machine-readable medium on a portable computing device adapted to present an augmented reality (AR) experience to a user about a physical article, the computer program comprising:

one or more software modules adapted to execute on the portable computing system and perform at least the following functions:

generate a graphical user interface (GUI) within the portable computing device adapted with a selectable enhanced content option enabling the user to engage with and render enhanced data within the GUI for a physical article associated with the wireless tag;

read a first enhanced experience wireless tag affixed to the physical article with a reader integrated within the portable computing device to determine a first enhanced experience wireless tag identification code;

communicate said first enhanced experience wireless tag identification code (TIC) with the portable computing device over a first network to a cloud-based server computing system as part of a request for enhanced experience content,

wherein said request further includes registration data verifying that the portable computing device is registered to receive first enhanced content for said first enhanced wireless tag identification code;

receive a first portion of a communications key for said first enhanced content over said first network at the portable computing device;

receive a second portion of a communications key for said first enhanced content over a second wireless network at the portable computing device;

reconstruct said first enhanced content at the portable computing device using both said first portion of said communications key and said second portion of said communications key; and

present said first enhanced content on the portable electronic device within the GUI as part of an enhanced presentation for the physical article.

33. A cloud computing system adapted to present enhanced content for a physical article through a secure channel to a portable computing device, comprising:

one or more software modules adapted to execute on computing hardware of the cloud computing system and perform at least the following functions:

a) associate a first physical article with first enhanced content, wherein the first enhanced content is configured to be presented within a graphical user interface (GUI) on the portable computing device for the first physical article;

b) associate a first enhanced content wireless tag with the first physical article, which first enhanced content wireless tag is coded with a first tag identification code (TIC);

c) process a request from the portable computing device received over a first network for said first enhanced content, said processing including performing a first verification of said TIC presented by the portable computing device within a tag payload, and a second verification of the portable computing device as registered to receive first enhanced content for said first enhanced wireless tag identification code;

d) generate and communicate a first partial portion of said first enhanced content to the portable communications device through the first network after said verifications; and

e) generate and communicate a second partial portion of said first enhanced content to the portable communications device though a separate second wireless network after said verifications, wherein said first enhanced content can be communicated securely and in a form that permits said first enhanced content to be reconstructed by a mobile application and presented on a graphical user interface (GUI) of the portable electronic device.

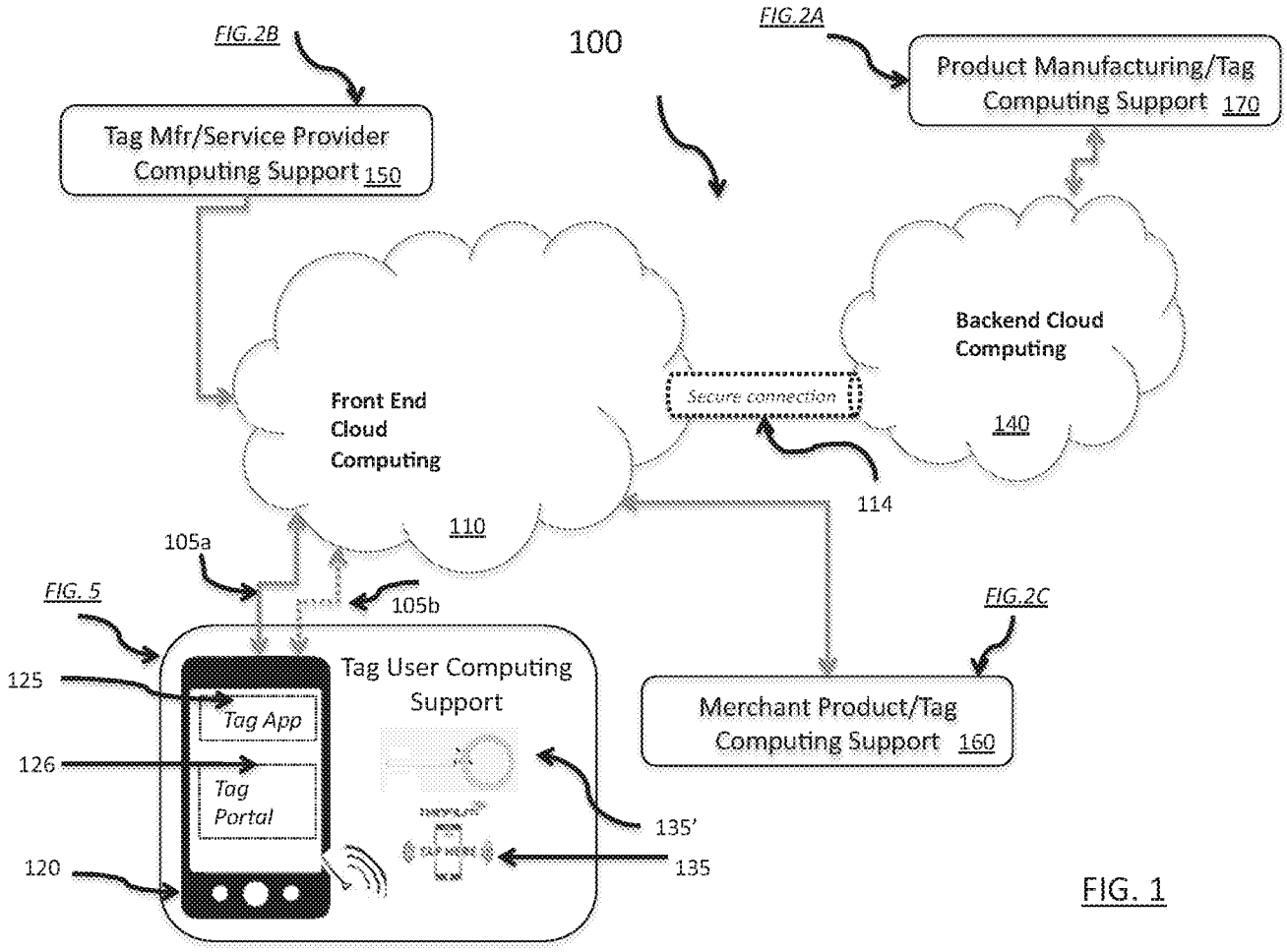
FIG.2B
100
FIG.2A
Tag Mfr/Service Provider Computing Support 150
Product Manufacturing/Tag Computing Support 170
Backend Cloud Computing
140
Front End Cloud Computing
110
Secure connection
114
105a
105b
FIG. 5
FIG.2C
125
126
120
Tag App
Tag Portal
Tag User Computing Support
Merchant Product/Tag Computing Support 160
135'
135

FIG. 1

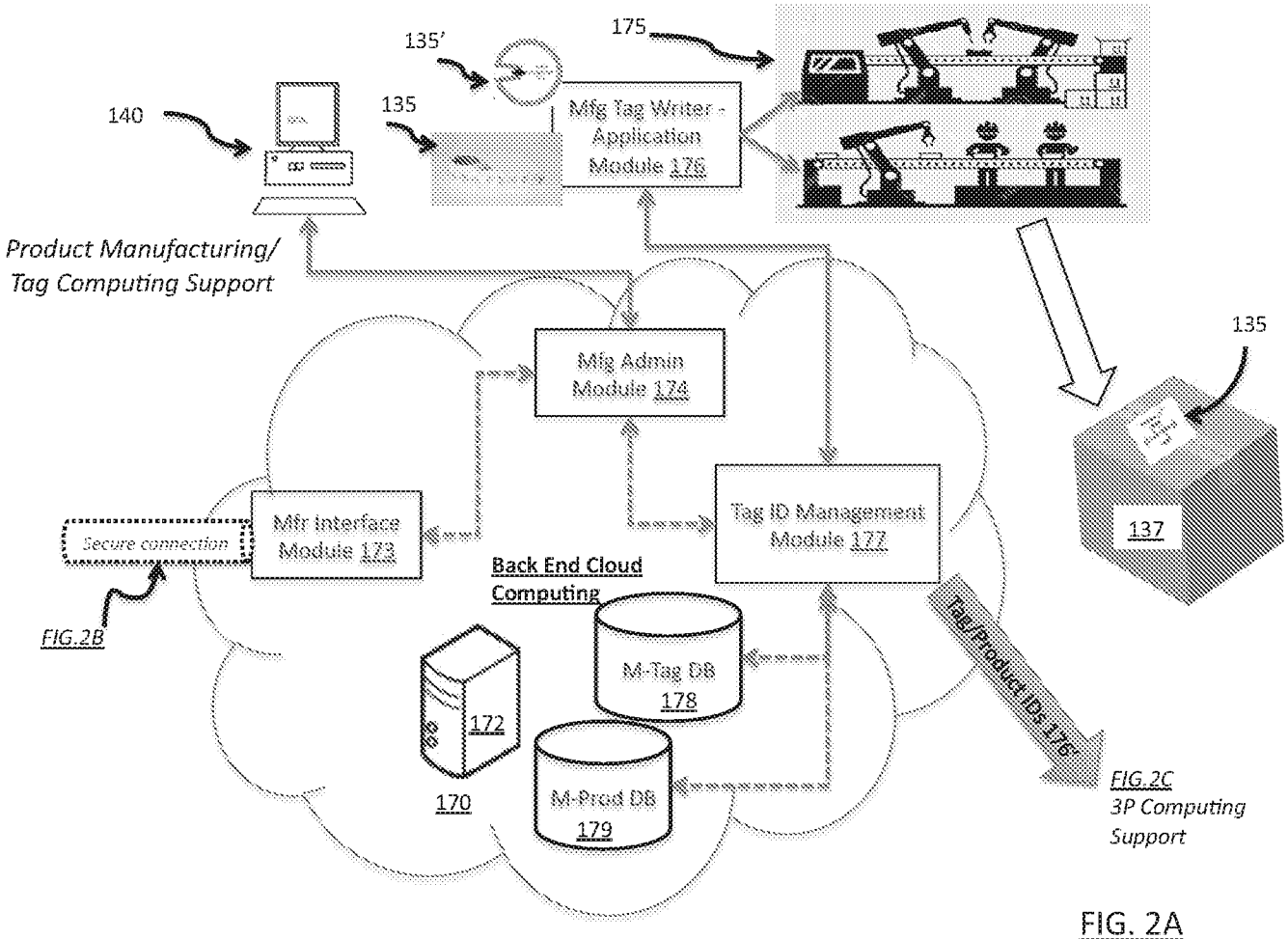
135'
175
140
135
Mfg Tag Writer - Application Module 176
Product Manufacturing/ Tag Computing Support
Mfg Admin Module 174
135
137
Mfr Interface Module 173
Secure connection
Tag ID Management Module 177
Back End Cloud Computing
FIG.2B
M-Tag DB 178
172
170
M-Prod DB 179
Tag/Product IDs 176
FIG.2C
3P Computing Support

FIG. 2A

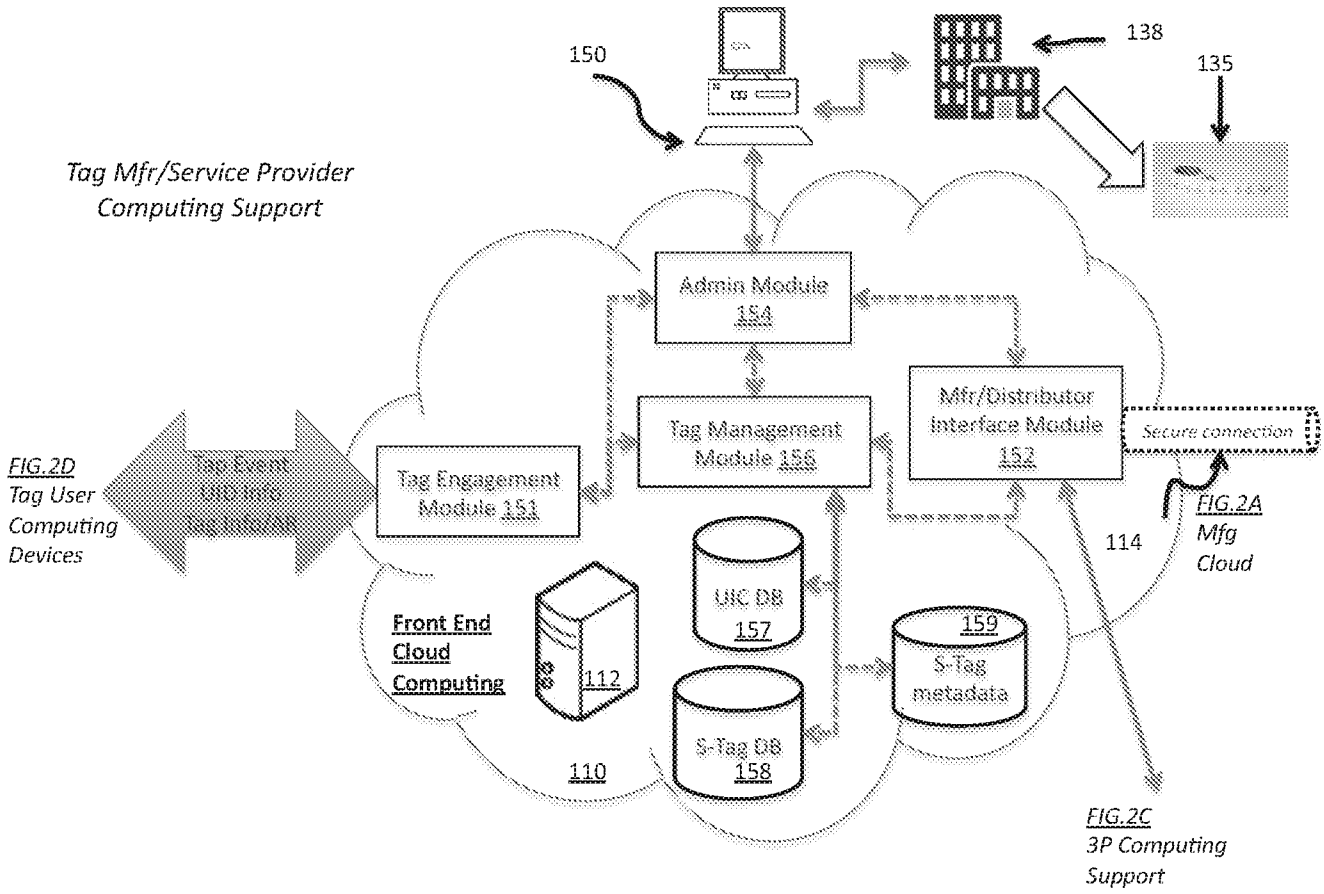
150
138
135
Tag Mfr/Service Provider
Computing Support
Admin Module
154
Tag Management
Module 156
Mfr/Distributor
Interface Module
152
Secure connection
FIG.2A
Mfg
Cloud
FIG.2D
Tag User
Computing
Devices
Tag Engagement
Module 151
114
Front End
Cloud
Computing
112
UIC DB
157
159
S-Tag
metadata
S-Tag DB
158
110
FIG.2C
3P Computing
Support

FIG. 2B

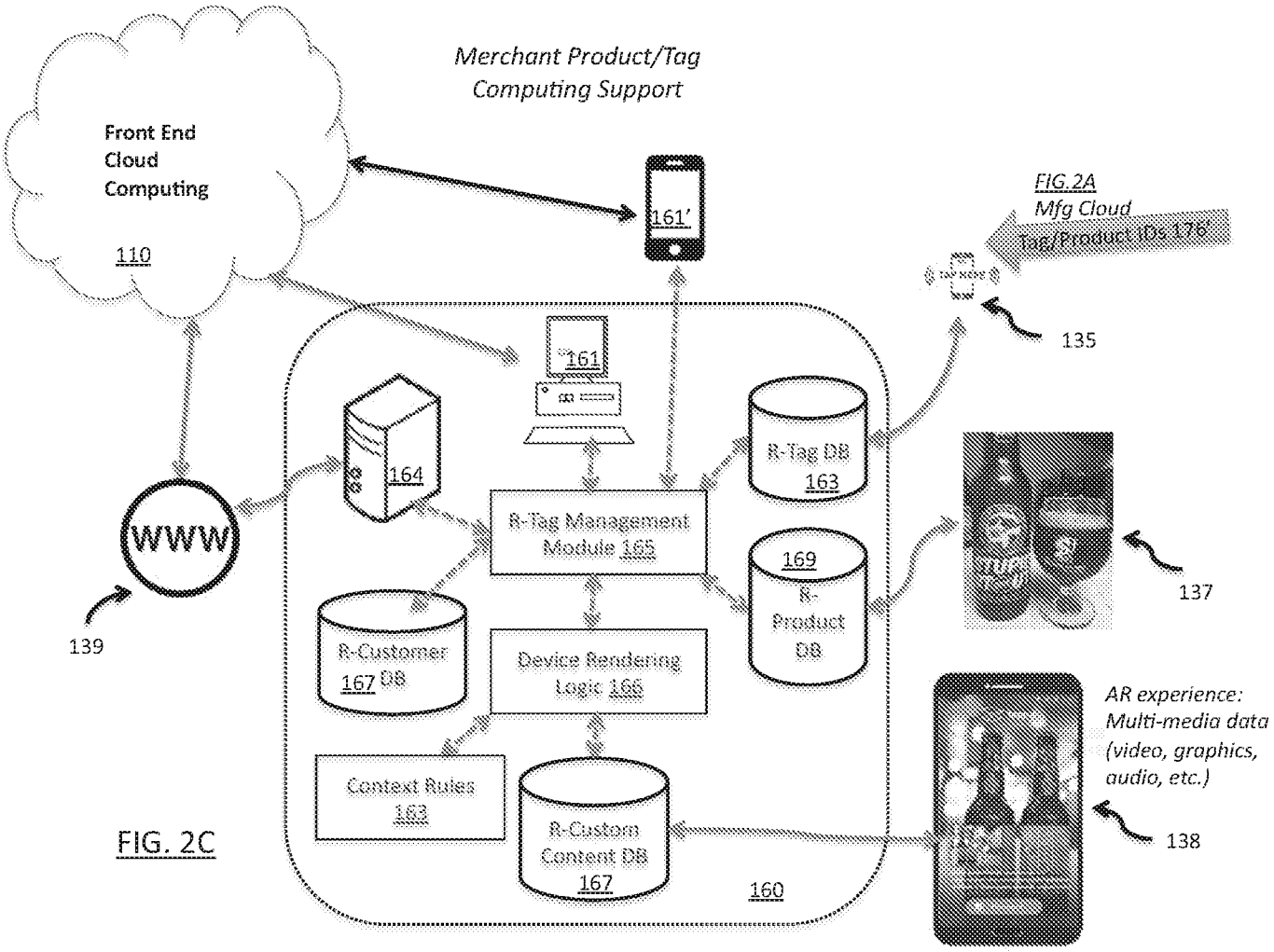
Front End
Cloud
Computing
110
Merchant Product/Tag
Computing Support
161'
FIG.2A
Mfg Cloud
Tag/Product IDs 176
135
161
164
WWW
139
R-Tag Management
Module 165
R-Tag DB
163
169
R-
Product
DB
137
R-Customer
167 DB
Device Rendering
Logic 166
Context Rules
163
R-Custom
Content DB
167
160
AR experience:
Multi-media data
(video, graphics,
audio, etc.)
138

FIG. 2C

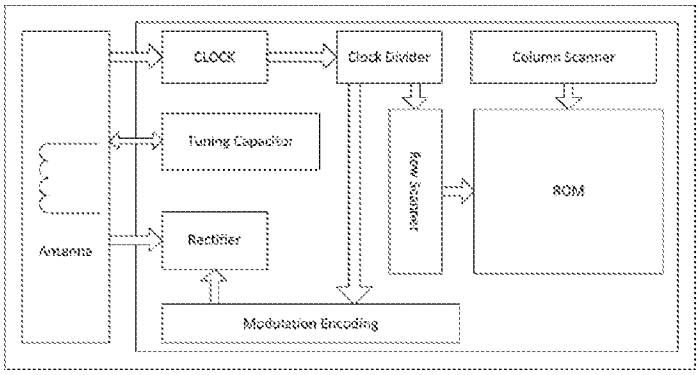

FIG. 3A

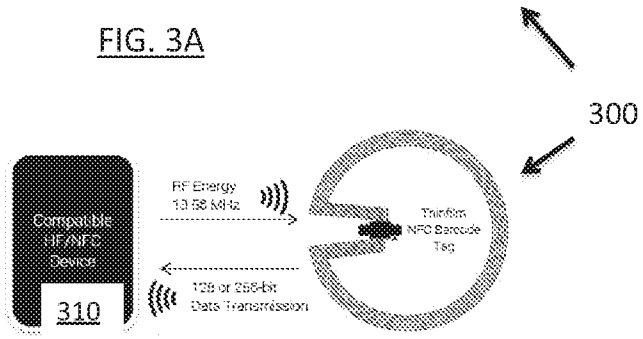

FIG. 3B

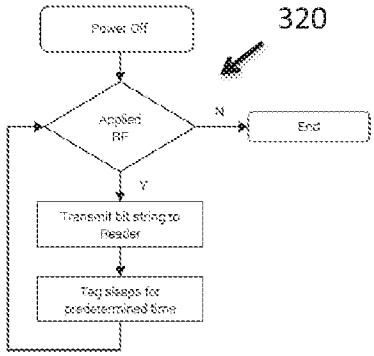

FIG. 3C

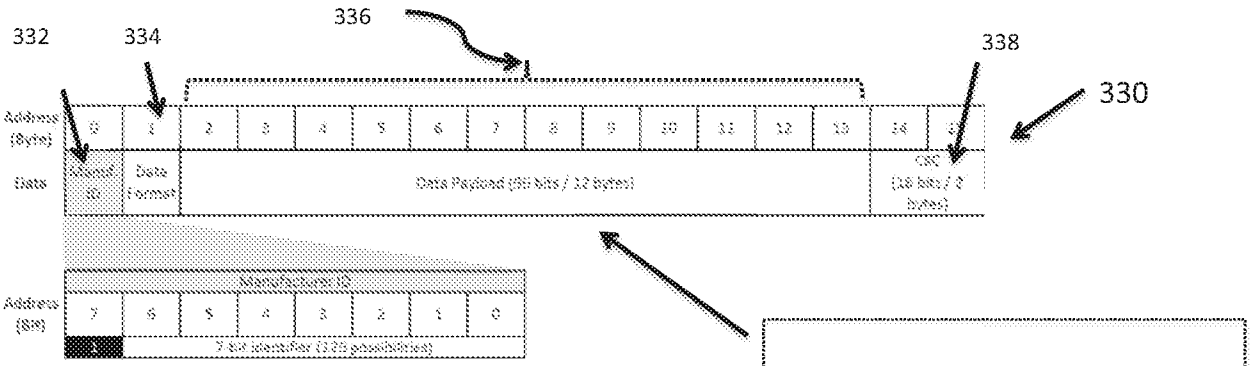

FIG. 3D

FIG. 3F

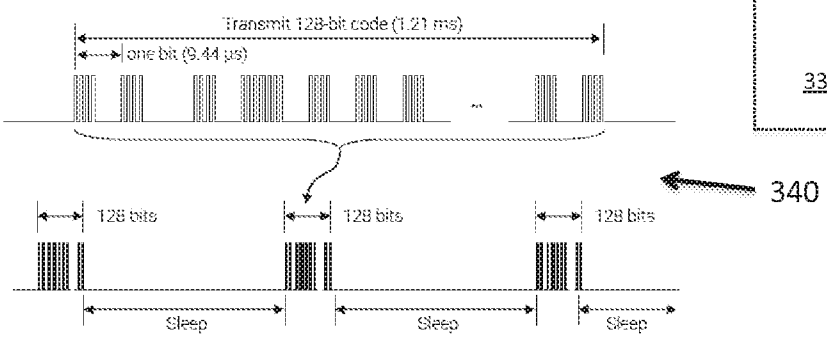

FIG. 3E

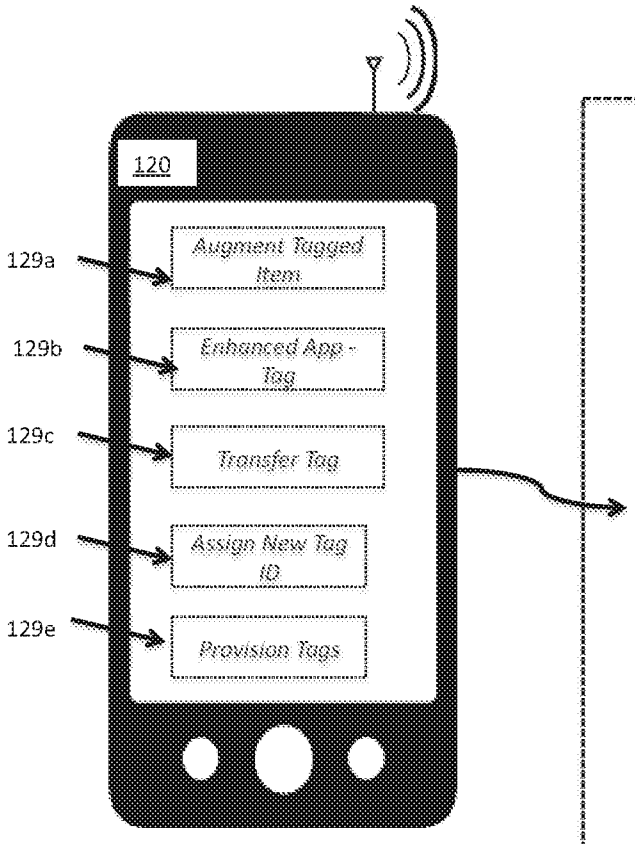
120
129a
Augment Tagged Item
129b
Enhanced App - Tag
129c
Transfer Tag
129d
Assign New Tag ID
129e
Provision Tags

FIG. 4B

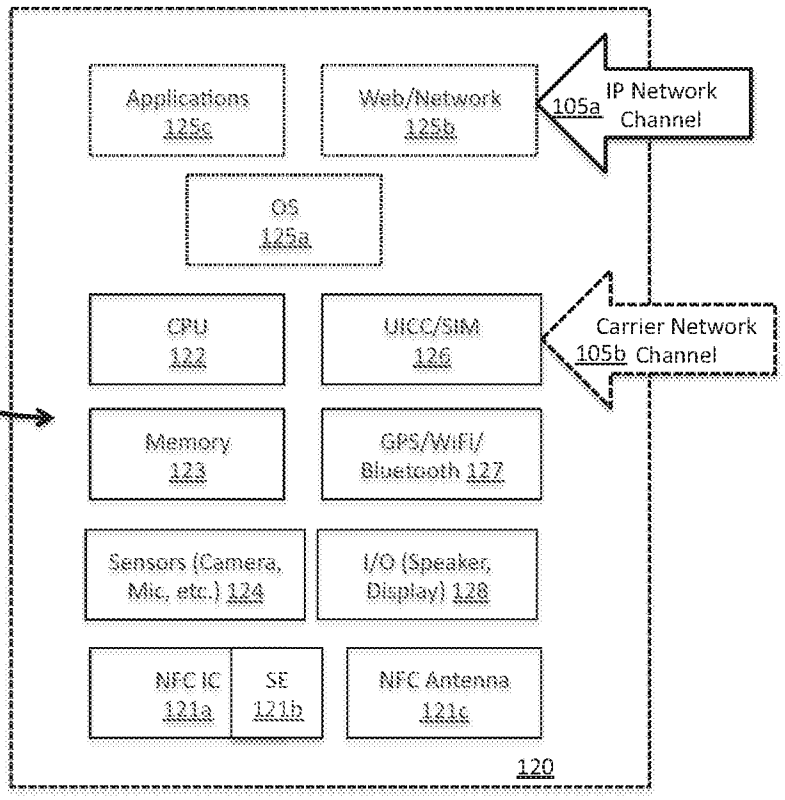
Applications 125c
Web/Network 125b
105a
IP Network Channel
OS 125a
CPU 122
UICC/SIM 126
Carrier Network 105b Channel
Memory 123
GPS/WiFi/ Bluetooth 127
Sensors (Camera, Mic, etc.) 124
I/O (Speaker, Display) 128
NFC IC 121a
SE 121b
NFC Antenna 121c
120

FIG. 4A

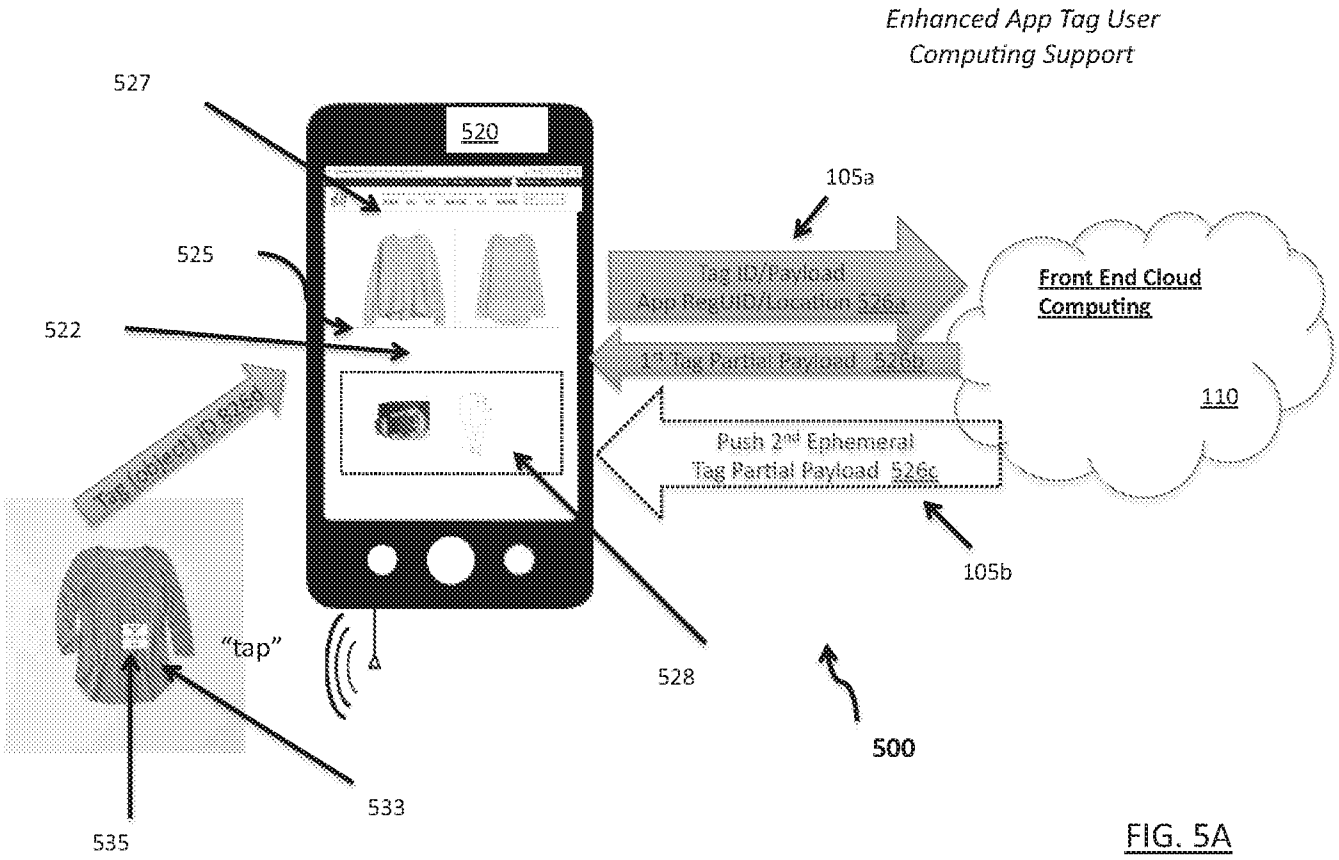
Enhanced App Tag User Computing Support
527
520
105a
525
522
Front End Cloud Computing
110
Push 2nd Ephemeral Tag Partial Payload 526c
105b
"tap"
528
500
533
535

FIG. 5A

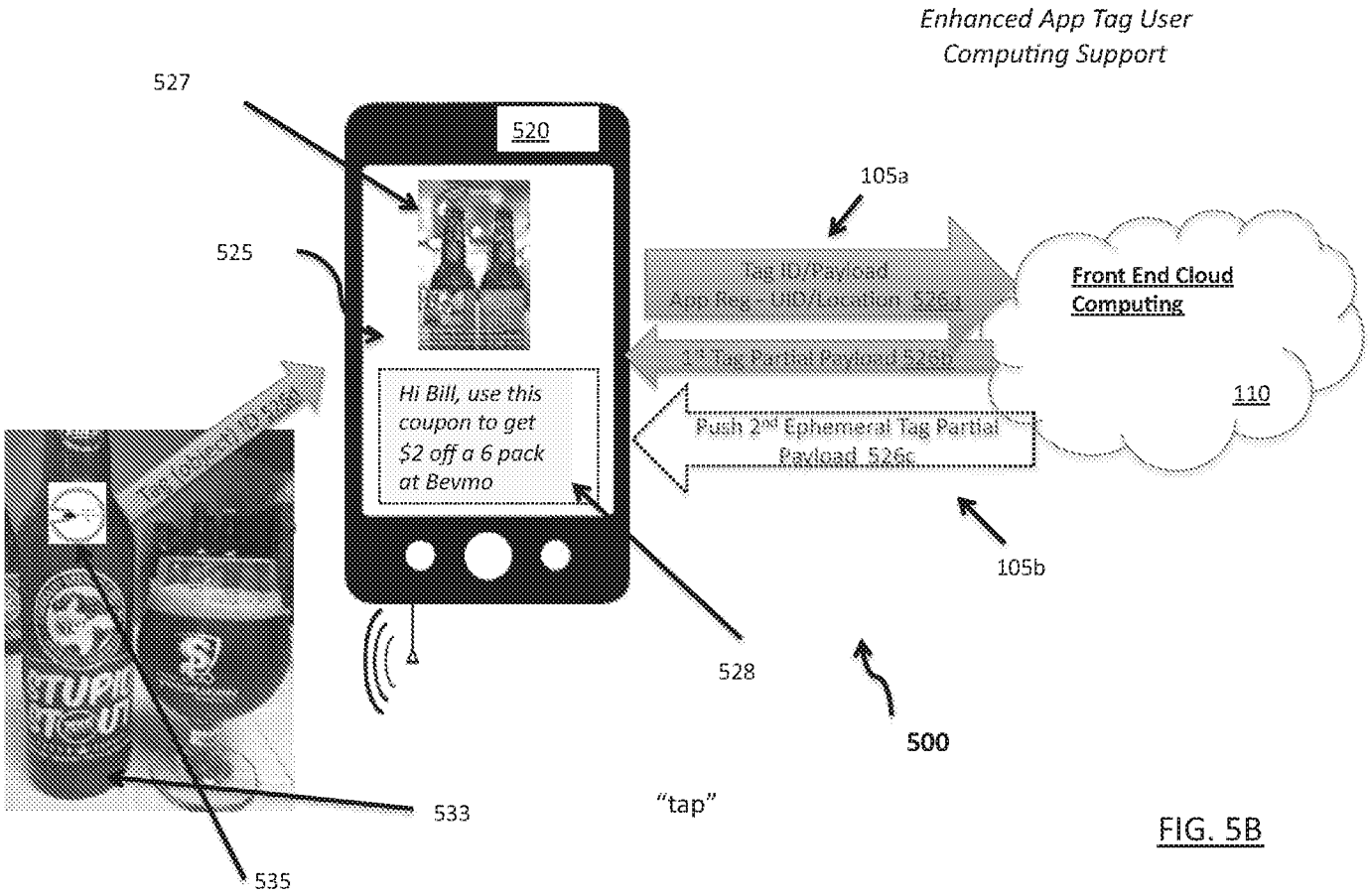
Enhanced App Tag User Computing Support
527
520
105a
525
Front End Cloud Computing
110
Hi Bill, use this coupon to get $2 off a 6 pack at Bevmo
Push 2nd Ephemeral Tag Partial Payload 526c
105b
528
500
533
"tap"
535

FIG. 5B

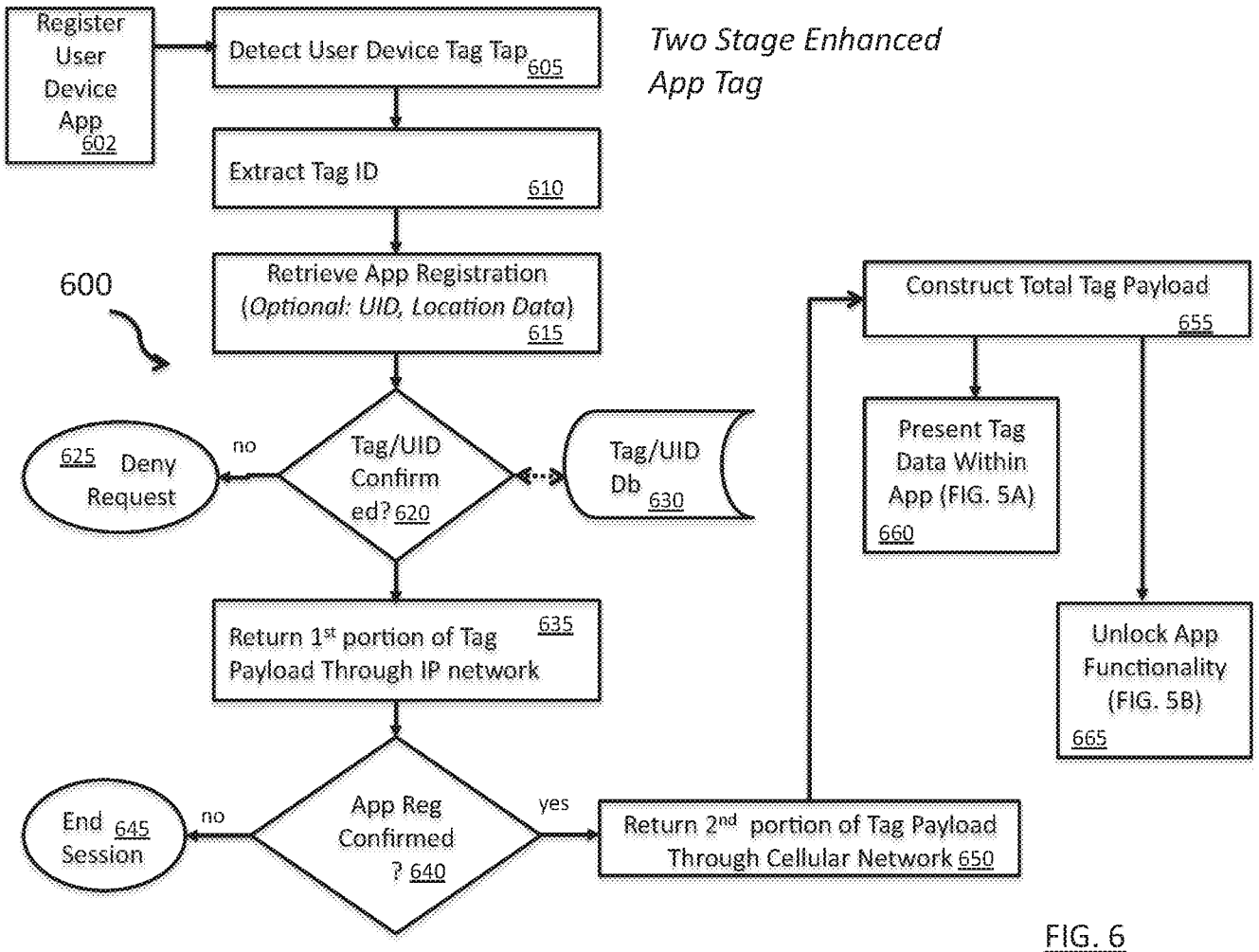
Register User Device App 602
Detect User Device Tag Tap 605
Two Stage Enhanced App Tag
Extract Tag ID 610
600
Retrieve App Registration (Optional: UID, Location Data) 615
Construct Total Tag Payload 655
Present Tag Data Within App (FIG. 5A) 660
625 Deny Request
no
Tag/UID Confirmed? 620
Tag/UID Db 630
Return 1st portion of Tag Payload Through IP network 635
Unlock App Functionality (FIG. 5B) 665
End 645 Session
no
App Reg Confirmed ? 640
yes
Return 2nd portion of Tag Payload Through Cellular Network 650

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 19/19397

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G07G 1/14; H04W 4/06; H04W 4/18 (2019.02)
CPC - G07G 1/0045; G07G 1/009; H04W 4/021; H04W 4/02; H04W 4/18; H04L 29/08; H04L 29/08081

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2013/0325594 A1 (MEHTA) 05 December 2013 (05.12.2013), entire document, especially; para [0005], [0007], [0019], [0025]	1-33
A	US 2017/0351504 A1 (AFERO, INC) 07 December 2017 (07.12.2017), entire document, especially; para [0001], [0097], [0100], [0243], [0248]	1-33
A	US 2013/0124482 A1 (ATAMNA et al.) 16 May 2013 (16.05.2013), entire document	1-33
A	US 2015/0019342 A1 (QUALCOMM INCORPORATED) 15 January 2015 (15.01.2015), entire document	1-33

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2019	23 MAY 2019

Name and mailing address of the ISA/US	Authorized officer:
Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774