US009271110B1

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

(10) **Patent No.: US 9,271,110 B1**
(45) **Date of Patent: Feb. 23, 2016**

(54) **LOCATION AWARENESS SESSION MANAGEMENT AND CROSS APPLICATION SESSION MANAGEMENT**

(75) Inventors: **David K. Fultz**, Raymore, MO (US); **Victor Anend Vijayakirthi**, Lenexa, KS (US)

(73) Assignee: **Sprint Communications Company L.P.**, Overland Park, KS (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 672 days.

(21) Appl. No.: **13/544,802**

(22) Filed: **Jul. 9, 2012**

(51) **Int. Cl.**

H04M 1/66	(2006.01)
H04W 4/02	(2009.01)
H04W 64/00	(2009.01)
H04W 24/00	(2009.01)

(52) **U.S. Cl.**
CPC ***H04W 4/02*** (2013.01); ***H04W 64/00*** (2013.01)

(58) **Field of Classification Search**
CPC H04W 4/02; H04W 64/00
USPC 455/411, 456.1, 456.2, 456.3
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,800,590	A	1/1989	Vaughan	
5,588,056	A	12/1996	Ganesan	
5,592,553	A	1/1997	Guski et al.	
5,661,807	A	8/1997	Guski et al.	
6,161,185	A	12/2000	Guthrie et al.	
6,178,508	B1	1/2001	Kaufman	
6,470,454	B1	10/2002	Challener et al.	
6,496,937	B1	12/2002	Ichihara	
6,601,175	B1	7/2003	Arnold et al.	
6,731,731	B1	5/2004	Ueshima	
7,836,407	B2	11/2010	Pettinati	
8,331,337	B2 *	12/2012	Kambe et al.	370/338
8,484,482	B1	7/2013	Cherukumudi et al.	
8,583,091	B1	11/2013	Delker et al.	
8,588,749	B1	11/2013	Sadhvani et al.	
8,737,965	B2 *	5/2014	McCown et al.	455/411
8,775,820	B1	7/2014	Freeburne	
8,886,925	B2	11/2014	Qureshi et al.	
2002/0178370	A1	11/2002	Gurevich et al.	
2003/0216143	A1	11/2003	Roese et al.	
2005/0015601	A1	1/2005	Tabi	
2005/0239481	A1	10/2005	Seligmann	

(Continued)

OTHER PUBLICATIONS

Paczkowski, Lyle W., et al., "Restricting Access of a Portable Communication Device to Confidential Data or Applications via a Remote Network Based on Event Triggers Generated by the Portable Communication Device", filed Mar. 15, 2013, U.S. Appl. No. 13/844,282.

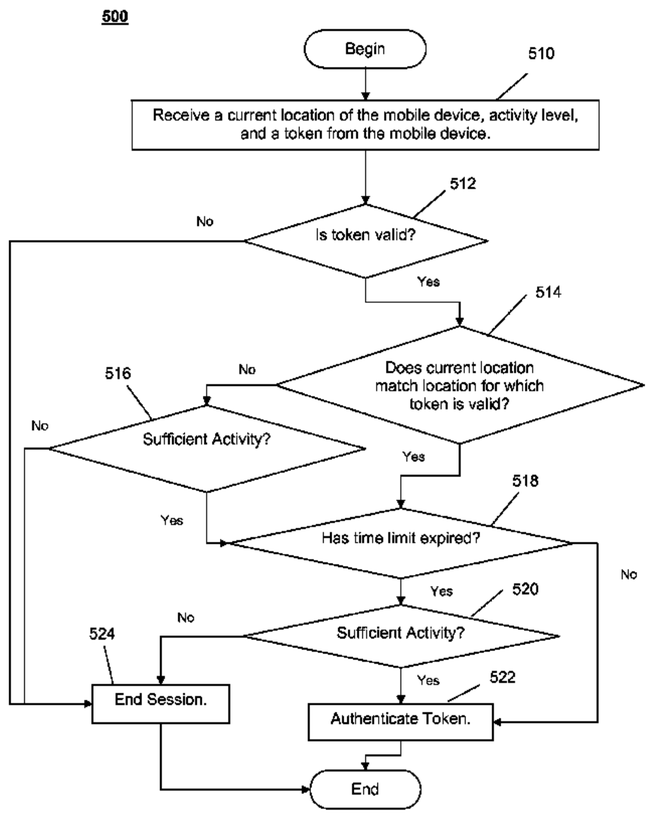
(Continued)

Primary Examiner — Muthuswamy Manoharan

(57) **ABSTRACT**

A location aware session token generation and validation system is provided. The system comprises a server system comprising at least one processor. The server system also comprises at least one non-transitory memory. The system further comprises a token component stored on the at least one non-transitory memory that, when executed by the server system, receives a request to initiate an application level session from a mobile device, wherein the request includes an identification of the mobile device and a location of the mobile device, generates a token for the application level session wherein the token is time limited and location limited such that the application level session will expire at the end of a specified period of time or when the mobile device moves from the location.

20 Claims, 9 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2005/0268345	A1	12/2005	Harrison et al.	
2005/0272445	A1	12/2005	Zellner	
2006/0212589	A1*	9/2006	Hayer et al.	709/229
2009/0047923	A1	2/2009	Jain et al.	
2010/0077487	A1	3/2010	Travis et al.	
2011/0072492	A1	3/2011	Mohler et al.	
2011/0166883	A1	7/2011	Palmer et al.	
2011/0208797	A1	8/2011	Kim	
2012/0136572	A1	5/2012	Norton	
2012/0154413	A1	6/2012	Kim et al.	
2013/0074067	A1	3/2013	Chowdhry	
2013/0097657	A1	4/2013	Cardamore et al.	
2013/0124583	A1	5/2013	Ferguson et al.	
2013/0252583	A1*	9/2013	Brown et al.	455/411
2013/0290709	A1	10/2013	Muppidi et al.	
2014/0007222	A1	1/2014	Qureshi et al.	
2014/0059642	A1	2/2014	Deasy et al.	
2014/0074508	A1	3/2014	Ying et al.	
2014/0173747	A1	6/2014	Govindaraju	

OTHER PUBLICATIONS

FAIPP Pre-Interview Communication dated Oct. 29, 2014, U.S. Appl. No. 13/844,282, filed Mar. 15, 2013.
Office Action dated Jun. 18, 2009, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Final Office Action dated Dec. 1, 2009, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Advisory Action dated Feb. 16, 2010, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Office Action dated Apr. 20, 2010, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Final Office Action dated Aug. 19, 2010, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Examiner's Answer dated Feb. 24, 2011, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Notice of Allowance dated Feb. 24, 2014, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
FAIPP Pre-Interview Communication dated Jan. 2, 2013, U.S. Appl. No. 13/042,015, filed Mar. 7, 2011.
Notice of Allowance dated Mar. 4, 2013, U.S. Appl. No. 13/042,015, filed Mar. 7, 2011.
Patent Board Decision, Examiner Reversed dated Nov. 22, 2013, U.S. Appl. No. 11/446,284, filed Jun. 2, 2006.
Final Office Action dated Mar. 24, 2015, U.S. Appl. No. 13/844,282, filed Mar. 15, 2013.
Advisory Action dated Jun. 10, 2015, U.S. Appl. No. 13/844,282, filed Mar. 15, 2013.
Office Action dated Aug. 24, 2015, U.S. Appl. No. 13/844,282, filed Mar. 15, 2013.

* cited by examiner

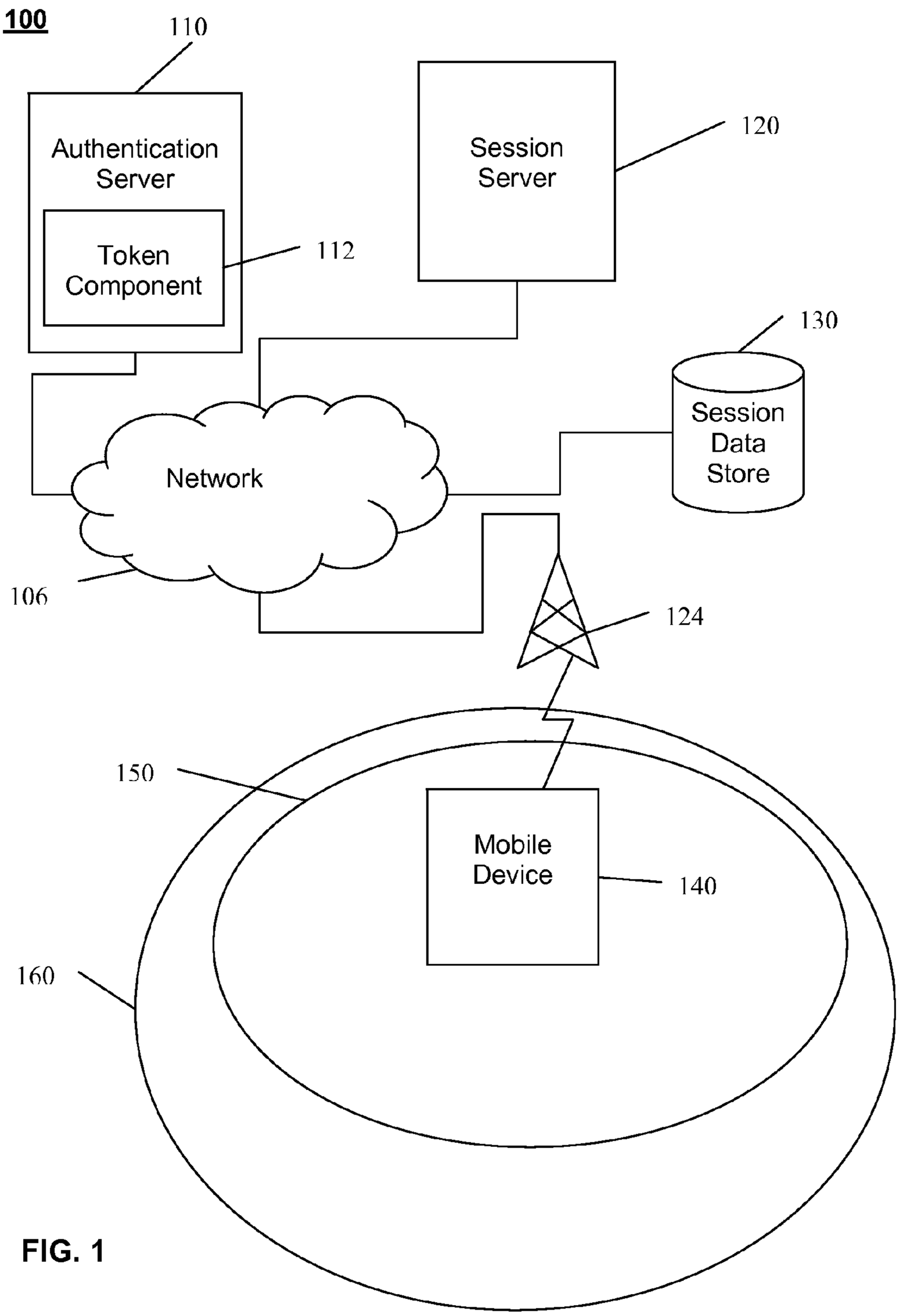

100
110
Authentication Server
Token Component
112
Session Server
120
130
Session Data Store
Network
106
124
150
Mobile Device
140
160

FIG. 1

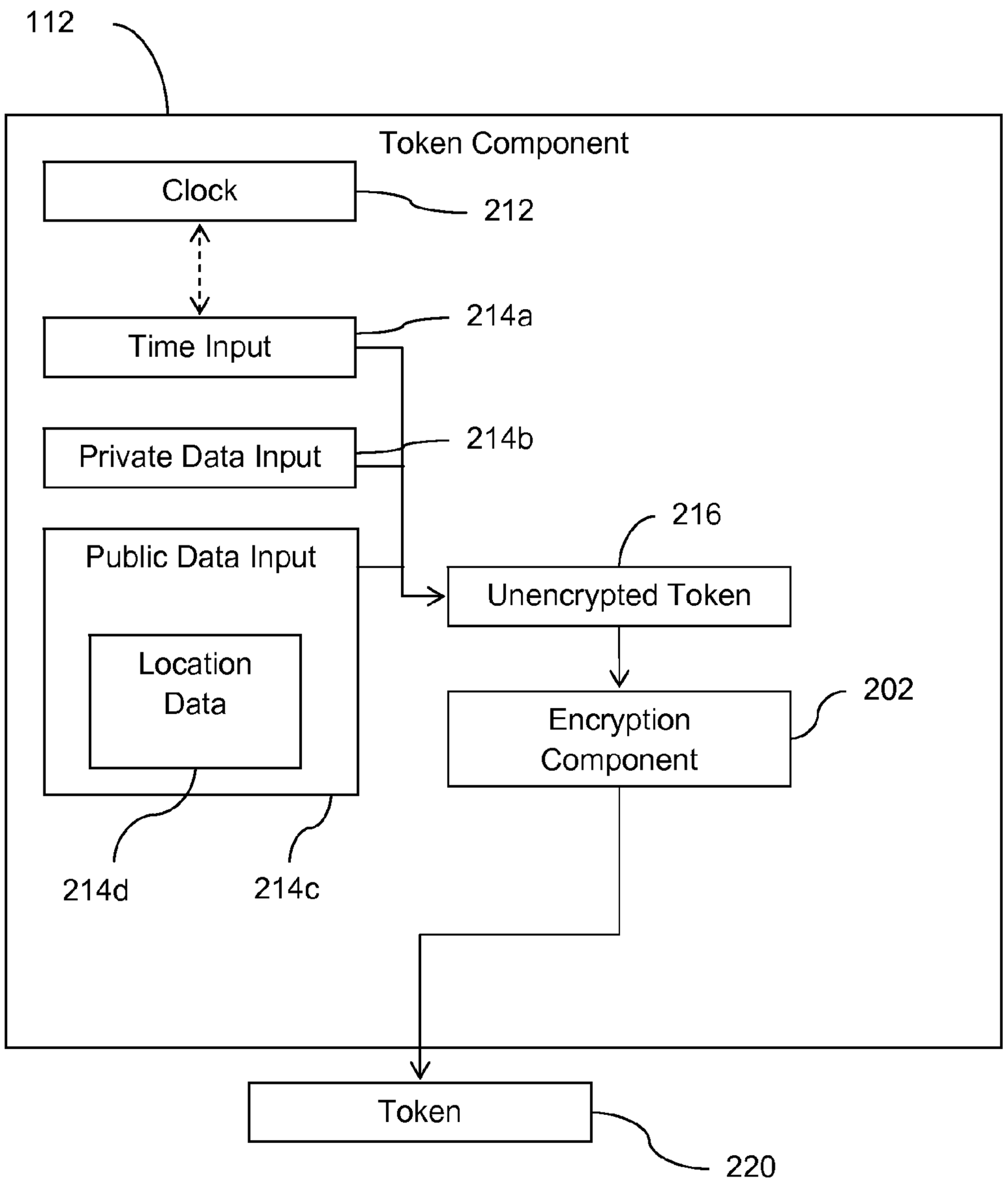

112
Token Component
Clock
212
Time Input
214a
Private Data Input
214b
Public Data Input
Location Data
214d
214c
216
Unencrypted Token
Encryption Component
202
Token
220

FIG. 2

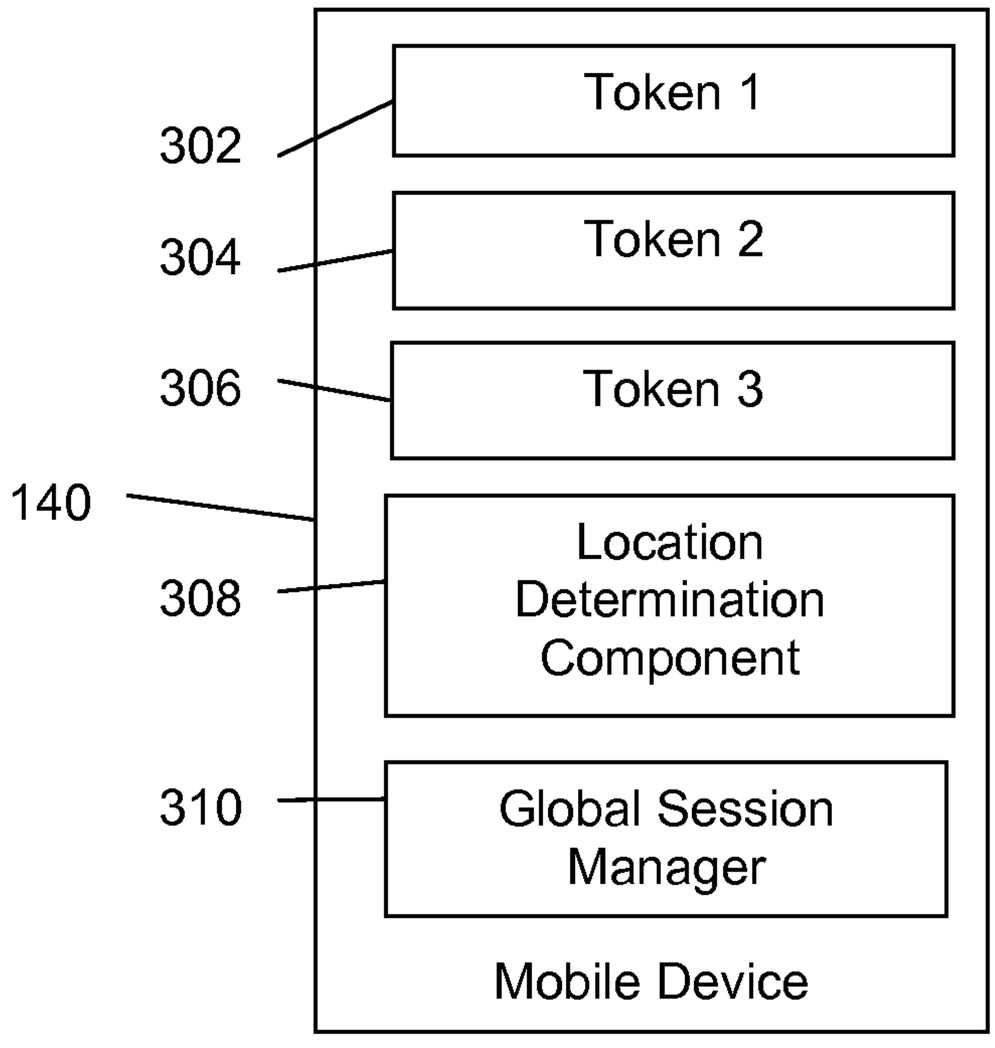

Token 1
302
Token 2
304
Token 3
306
140
Location Determination Component
308
Global Session Manager
310
Mobile Device

FIG. 3

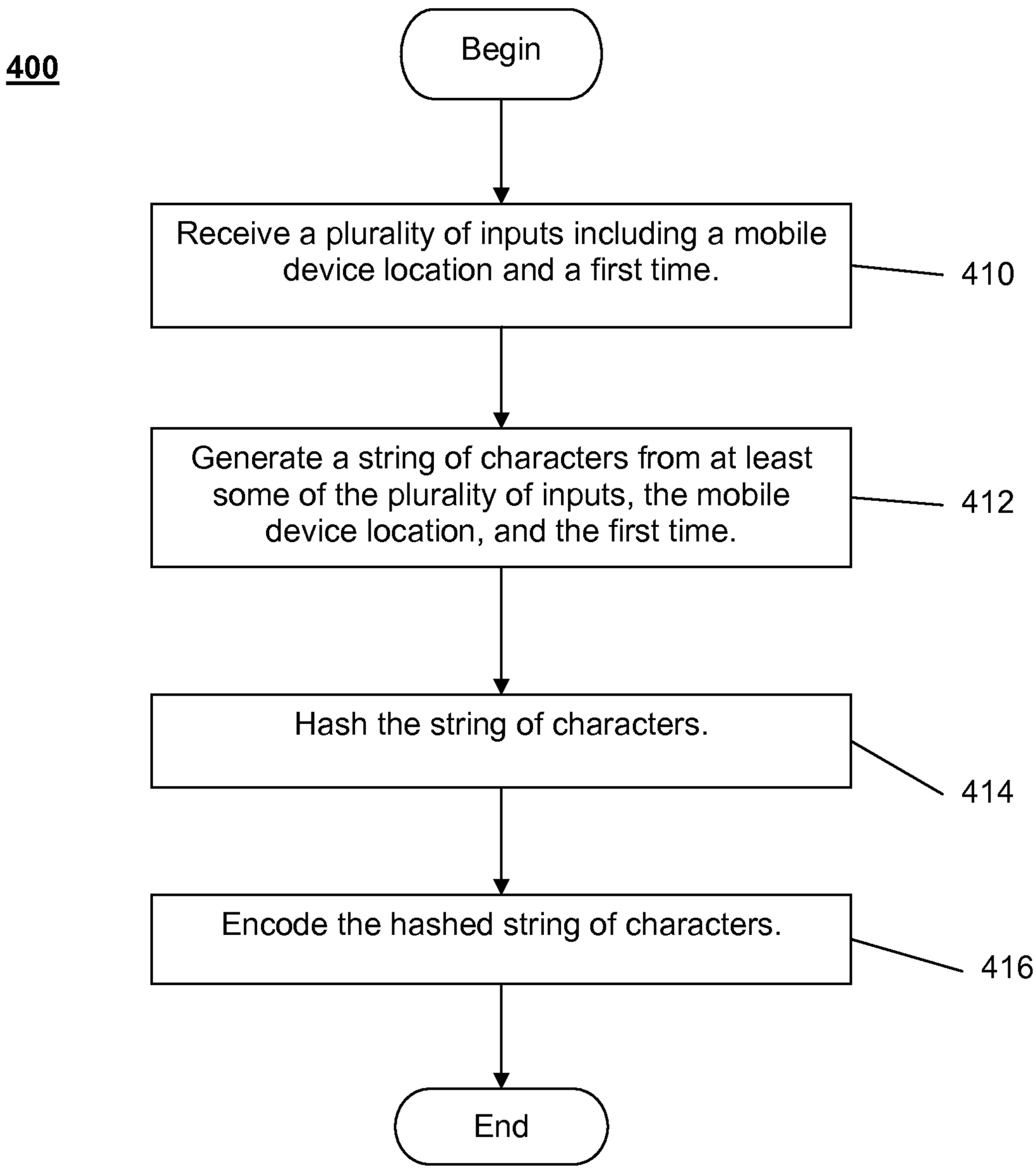

400
Begin
Receive a plurality of inputs including a mobile device location and a first time.
410
Generate a string of characters from at least some of the plurality of inputs, the mobile device location, and the first time.
412
Hash the string of characters.
414
Encode the hashed string of characters.
416
End

FIG. 4

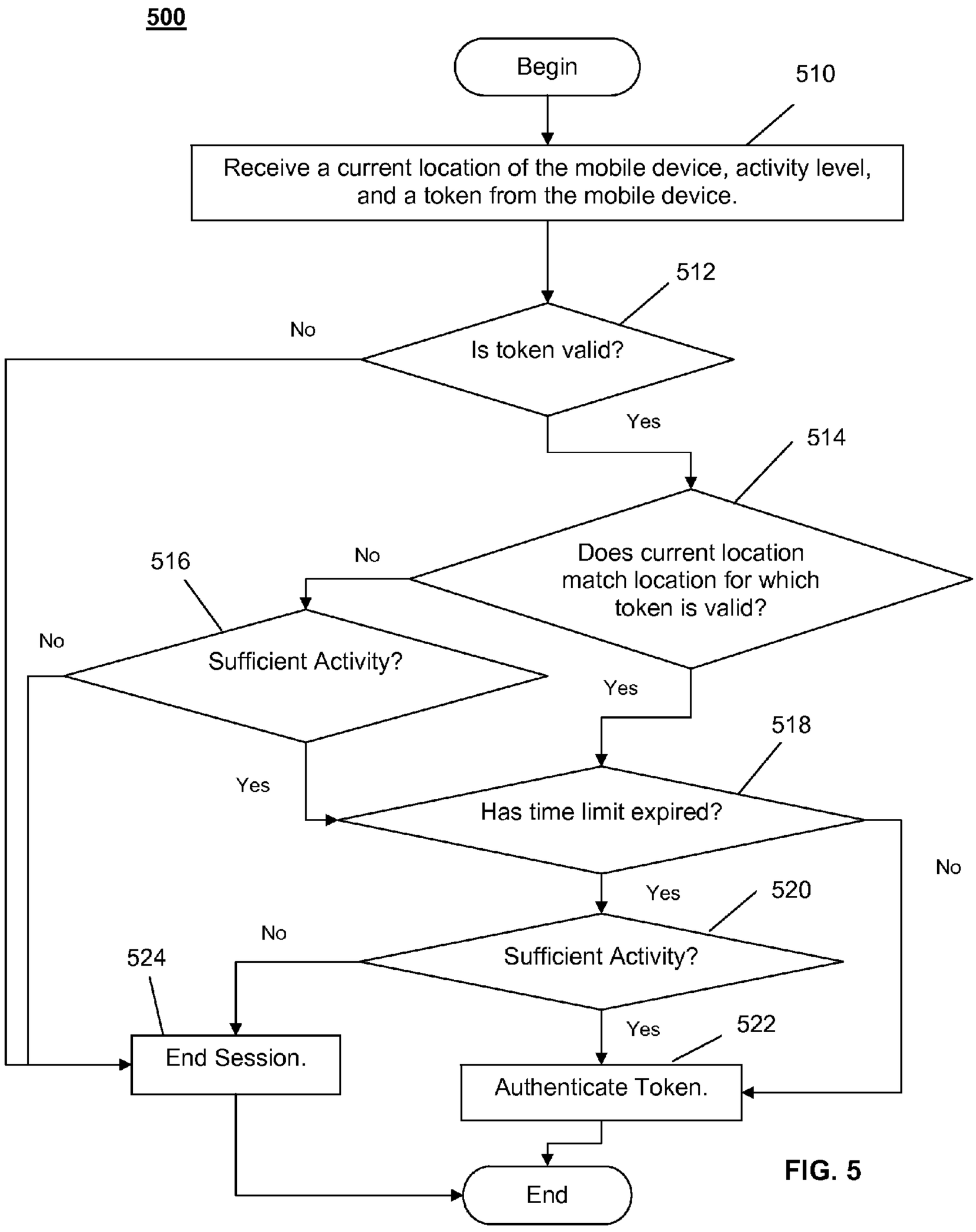

500
Begin
510
Receive a current location of the mobile device, activity level, and a token from the mobile device.
512
Is token valid?
No
Yes
514
Does current location match location for which token is valid?
No
516
Sufficient Activity?
No
Yes
518
Has time limit expired?
Yes
No
520
Sufficient Activity?
No
524
End Session.
Yes
522
Authenticate Token.
End

FIG. 5

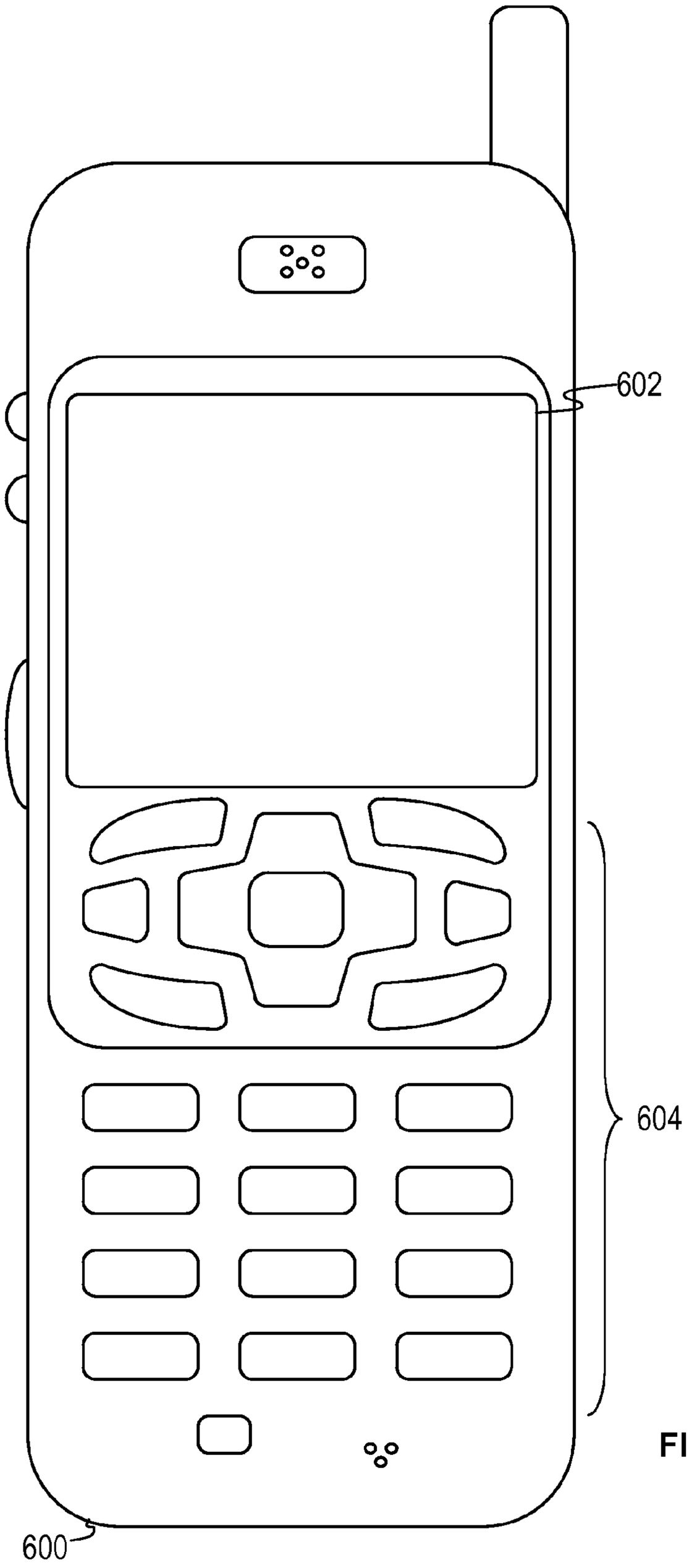


FIG. 6

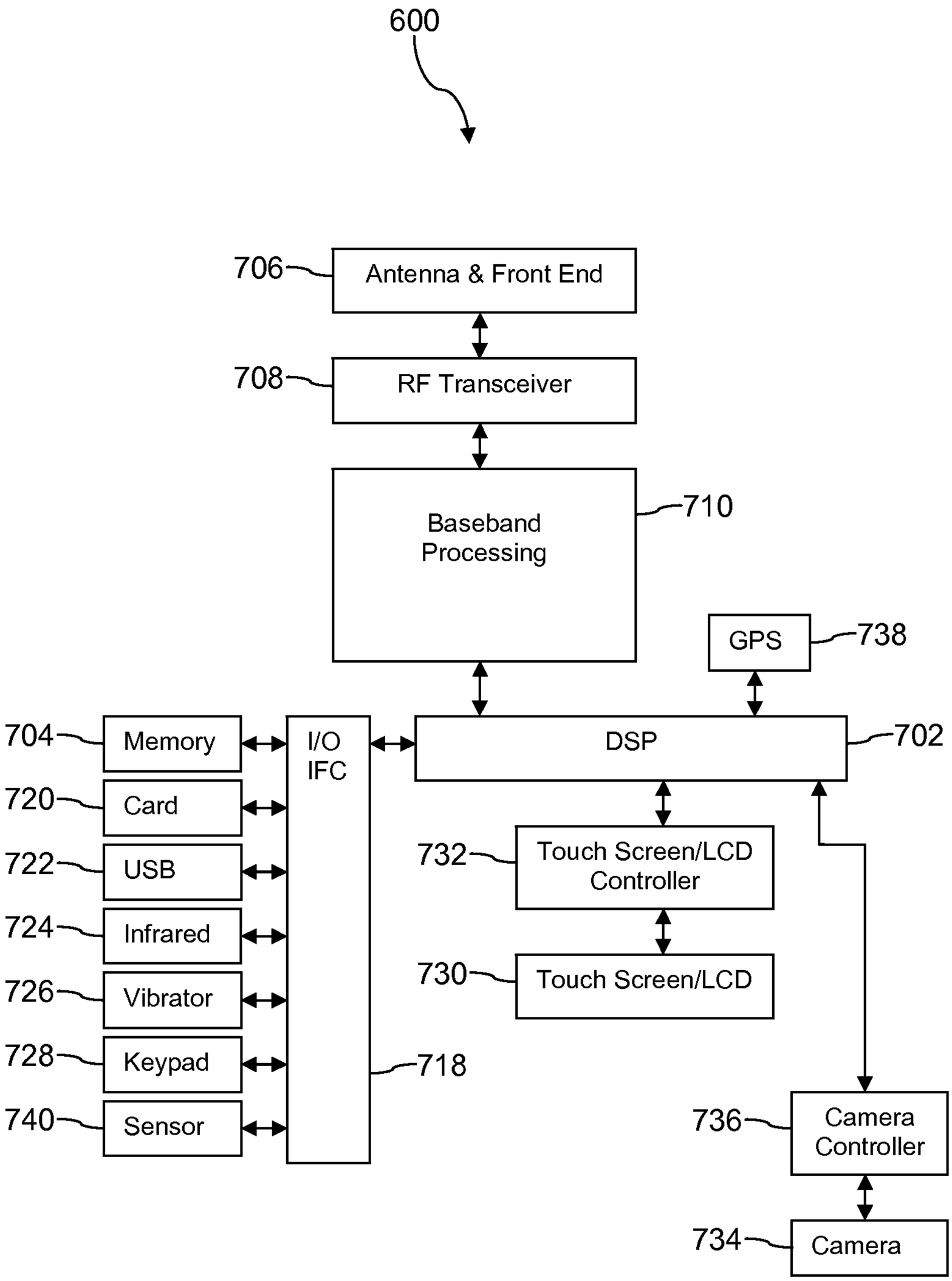

600
706
Antenna & Front End
708
RF Transceiver
Baseband Processing
710
GPS
738
704
Memory
720
Card
722
USB
724
Infrared
726
Vibrator
728
Keypad
740
Sensor
I/O IFC
718
DSP
702
732
Touch Screen/LCD Controller
730
Touch Screen/LCD
736
Camera Controller
734
Camera

FIG. 7

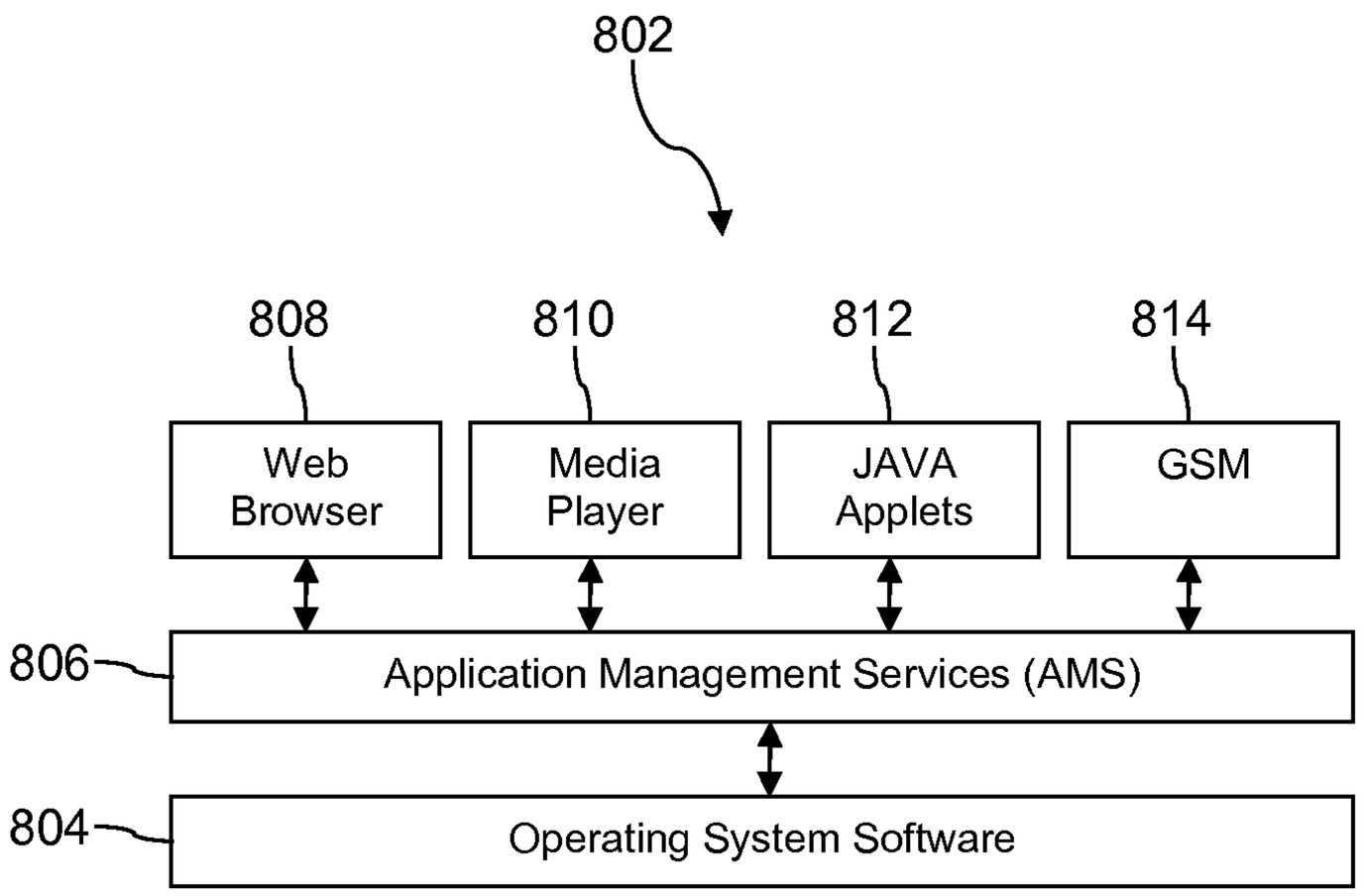

802
808
810
812
814
Web Browser
Media Player
JAVA Applets
GSM
806
Application Management Services (AMS)
804
Operating System Software

FIG. 8A

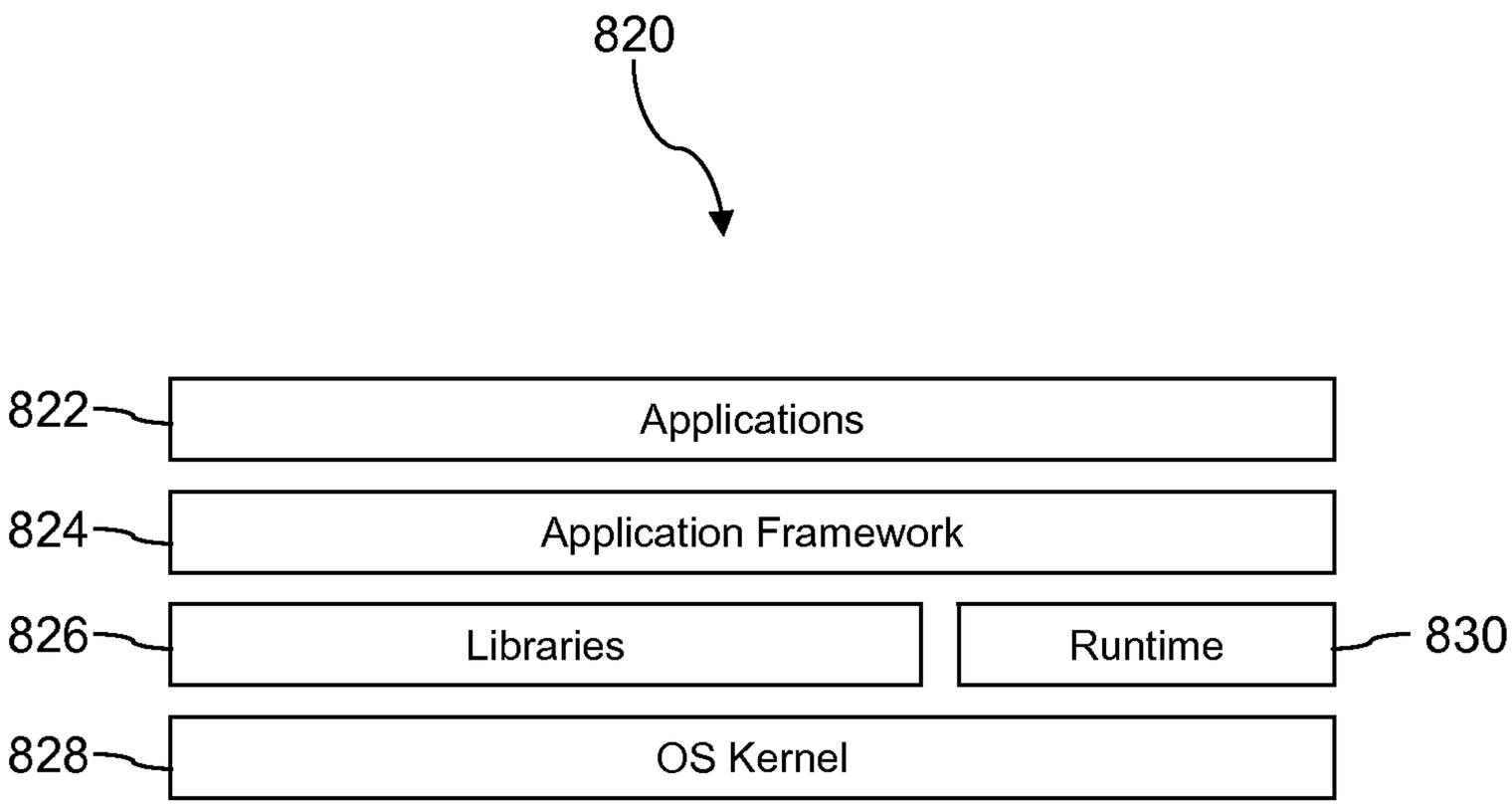

820
822
Applications
824
Application Framework
826
Libraries
Runtime
830
828
OS Kernel

FIG. 8B

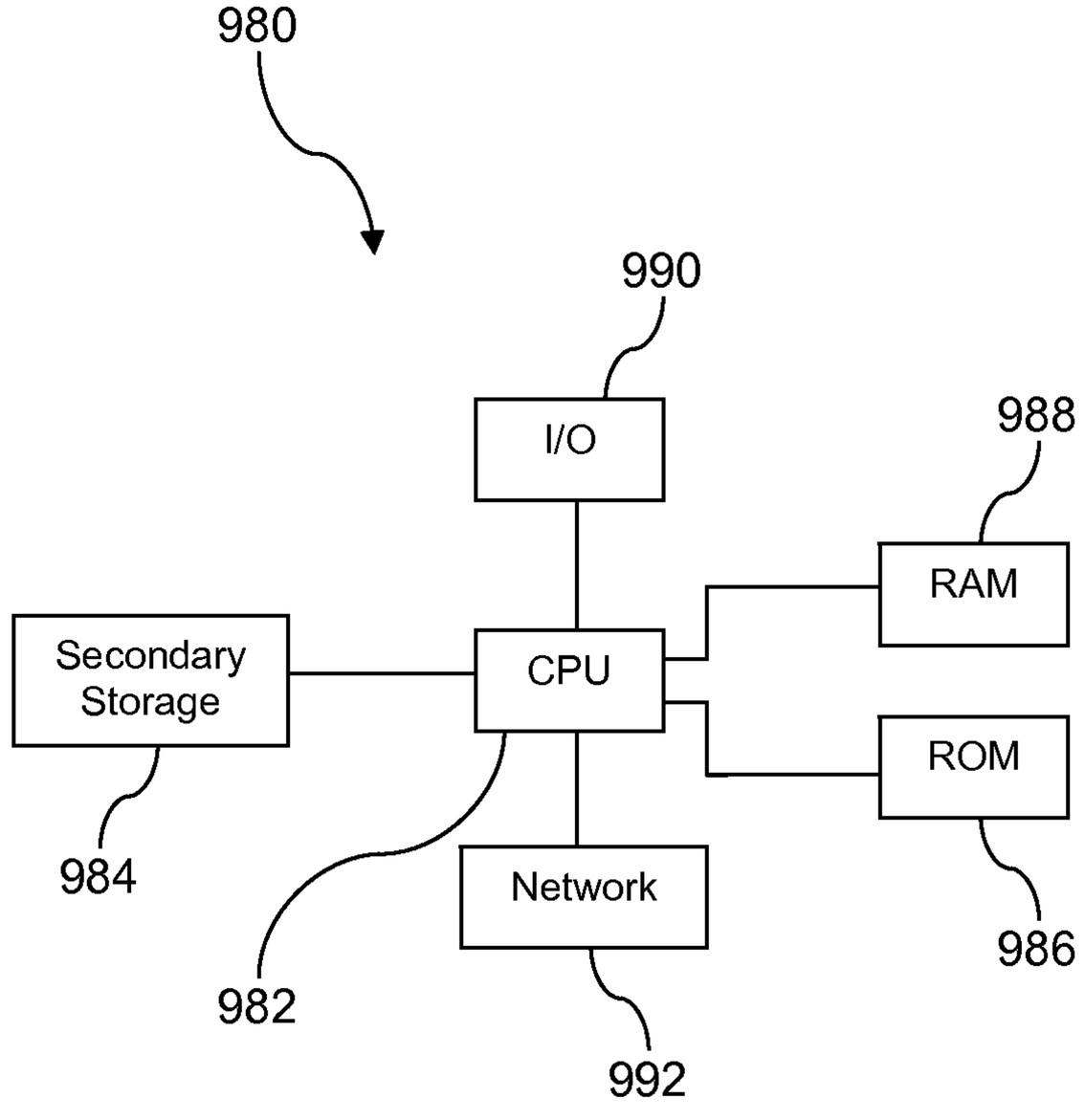

980
990
I/O
988
RAM
Secondary Storage
CPU
ROM
984
Network
986
982
992

FIG. 9

LOCATION AWARENESS SESSION MANAGEMENT AND CROSS APPLICATION SESSION MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATIONS

None.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable.

REFERENCE TO A MICROFICHE APPENDIX

Not applicable.

BACKGROUND

In today's world, information security is a fundamental concern. Tokens are often used to promote information security by providing authentication and managing secure sessions. For example, a token may be used to prove identity or to gain access to a resource.

SUMMARY

In an embodiment, a location aware session token generation and validation system is provided. The system comprises a server system comprising at least one processor. The system also comprises at least one non-transitory memory. The system further comprises a token component stored on the at least one non-transitory memory that, when executed by the server system, receives a request to initiate an application level session from a mobile device, wherein the request includes an identification of the mobile device and a location of the mobile device, generates a token for the application level session wherein the token is time limited and location limited such that the application level session will expire at the end of a specified period of time or when the mobile device moves from the location, sends the token to the mobile device, receives a session message from the mobile device, wherein the session message includes a requested session action, a current location of the mobile device and the token, analyzes the token, performs the requested session action when the specified period of time has not expired and if the current location matches the location, and ends the application level session if the specified period of time has expired or if the current location does not match the location.

In an embodiment, a cross application session management system for a mobile device is provided. The system comprises at least one processor and at least one non-transitory memory. The system also comprises a plurality of tokens stored on the at least one non-transitory memory, wherein each of the plurality of tokens corresponds to a respective one of a plurality of application level sessions. The system further comprises a global session management component stored on the at least one memory that, when executed by the at least one processor, monitors activity on the plurality of application level sessions, wherein activity on one of the plurality of application level sessions maintains the session life for the other ones of the plurality of application level sessions.

In an embodiment, a method for session management on a mobile device is provided. The method comprises receiving at an authenticating server a request for a token to authenticate an application level session with a service provider, wherein the request includes an identification of the mobile device and a location of the mobile device, generating by the authenticating server a token for the application level session wherein the token is time limited and location limited, sending the token to the mobile device, receiving at the authenticating server a session message for the application level session from the mobile device, wherein the session message includes a requested session action for the application level session, a current location of the mobile device, an activity level, and the token, and performing the requested session action when the predefined period of time has not expired and the current location does not match the location and the activity level exceeds a predefined level of activity.

These and other features will be more clearly understood from the following detailed description taken in conjunction with the accompanying drawings and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present disclosure, reference is now made to the following brief description, taken in connection with the accompanying drawings and detailed description, wherein like reference numerals represent like parts.

FIG. **1** is a block diagram of a system according to an embodiment of the disclosure.

FIG. **2** is a block diagram a token component according to an embodiment of the disclosure.

FIG. **3**, a block diagram of a mobile device according to an embodiment of the disclosure.

FIG. **4** is a flowchart of a method for generating a token according to an embodiment of the disclosure.

FIG. **5** is a flowchart of a method for validating a token according to an embodiment of the disclosure.

FIG. **6** is a pictorial diagram of a mobile device according to an embodiment of the disclosure.

FIG. **7** is a block diagram of a mobile device according to an embodiment of the disclosure.

FIG. **8**A illustrates a software environment for a mobile device according to an embodiment of the disclosure.

FIG. **8**B illustrates an alternative software environment for a mobile device according to an embodiment of the disclosure.

FIG. **9** illustrates an exemplary computer system suitable for implementing some aspects of the several embodiments of the disclosure.

DETAILED DESCRIPTION

It should be understood at the outset that although illustrative implementations of one or more embodiments are illustrated below, the disclosed systems and methods may be implemented using any number of techniques, whether currently known or not yet in existence. The disclosure should in no way be limited to the illustrative implementations, drawings, and techniques illustrated below, but may be modified within the scope of the appended claims along with their full scope of equivalents.

The present disclosure provides systems and methods for location awareness session management and cross application session management. A session may be a semi-permanent application level interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and a mobile device. An application level session is set up or established at a certain point in time, and ended or torn down at a later point in time. An established application

level communication session may involve more than one message in each direction. In order to prolong sessions and allow users of mobile devices greater freedom, in an embodiment, the present disclosure provides that an application level session is both time limited and location limited. However, by limiting the location of the mobile device in which the session is valid, the system promotes a service provider to increase the amount of time the application level session is valid above what the service provider might otherwise be comfortable with. For example, in an embodiment, as long as the mobile device is within the same location for which the application level session was initiated, the service provider may be more comfortable that the mobile device is still in possession of the user and has not been stolen allowing access to an unauthorized person. Thus, in such circumstances, the service provider may be willing to keep the application level session alive for a longer period of time. In an embodiment, if the mobile device moves outside of a specified location, the application level session may end. Moving the mobile device outside of the specified location may indicate that the device may have been stolen and no longer in the possession of the authorized user. In such case, by ending the application level session, fraudulent activity may be inhibited.

The mobile device may send an indication of its current location in each of its session messages. Alternatively, the mobile device may periodically send a distinct current location message to the service provider and/or to a session management server computer or session server. In an embodiment, the location of the mobile device may be determined based on a Global Positioning System (GPS), and the indication of current location that is sent by the mobile device may comprise GPS coordinates.

However, the disclosed systems and methods are not limited to GPS based location determination. In another embodiment, the location of the mobile device may be determined based on an available Worldwide Interoperability for Microwave Access (WiMAX) access point, an available WiFi access point, an available femtocell access point; or other available wireless access points regardless of whether the mobile device is actually connected to the available wireless access point. For example, the mobile device may receive a broadcast signal from a wireless access point that contains an identifier for the subject access point. In this case, the indication of current location that is sent by the mobile device may comprise an identity of one access point, identities of a plurality of access points, or other information about what wireless access points are in range of the mobile device. The service provider may deem that the mobile device is within an acceptable proximity of a preferred location, such as a retail store location, if the mobile device is in range of one or more predefined wireless access points, where the subject predefined wireless access points are associated with their identities. In an embodiment, the location of the mobile device may be determined based on triangulation of the strength of signals between a plurality of available wireless access points. In an embodiment, the location may be determined based on using combinations of different types of location determination methods. As such, the disclosed methods and systems are not limited to a particular method of determining the location of the mobile device.

In an embodiment, continuing activity or activity exceeding a predetermined threshold may prevent the application level session from being ended even though the mobile device may have moved outside of a specified location. The continuing activity may be taken as an indication that the mobile device is still in the possession of an authorized user and has not been stolen. Thus, continuing the session may be warranted. By continuing the session, the user experience is enhanced since they do not experience the frustration of being disconnected from their session and having to reestablish their session by entering, for example, a user name and password.

In an embodiment, cross application session awareness may provide that activity on one application or session may be sufficient to ensure that another session is not ended. For example, a bank may have enabled a session for a banking customer to access the customer's bank account information. The customer may need to check information in an e-mail as well as access confidential information on another web site through a session on the other web site. For example, the customer may need to access a web site associated with their credit card issuer to locate additional information before completing their session with their bank. Their online session with their bank may have been idle for a significant amount of time that would normally result in the session being ended. However, a trusted global session manager may monitor session and application activity across multiple sessions and/or applications. In such circumstances, the customer's activity on their e-mail and on their credit card issuer's web site may be sufficient to keep their session with their bank active. Such activity may indicate that the customer has not left their mobile device and is still in possession of the device making it unlikely that unauthorized access to the customer's bank account may be granted by keeping the session alive.

In an embodiment, to manage sessions, a token may be generated based on a current location of a mobile device. The token may be provided to the mobile device and provided with all messages transmitted from the mobile device to a session server. A token may be any data used to uniquely identify an individual and/or device and authenticate that individual and/or device for a session. In an embodiment, a token may be a string of characters. In an embodiment, a token may be a cookie, which may also be referred to as an HTTP cookie, a web cookie, or a browser cookie. In an embodiment, the token is a self-expiring token that may end a session after the expiration of a specified amount of time.

Turning now to FIG. **1**, a system **100** for location awareness session management and cross application session management is provided. In an embodiment, the system **100** comprises mobile devices **140**, a base transceiver station **124**, an authentication server **110**, a session server **120**, a session data store **130**, and a network **106**. Although shown as two separate machines, authentication server **110** and session server **120** may be implemented on different machines or on the same machine.

In an embodiment, mobile device **140** may be any portable electronic device including a mobile phone, a personal digital assistant (PDA), a smart phone, a tablet computer, and a laptop computer. A smart phone may be a mobile device that includes not only the traditional features of a mobile phone, but also additional functionality such as, for example, providing e-mail service, web access, and still picture and video capture capability via a camera. A smart phone may also run applications including games and productivity applications. Examples of mobile devices include an Android™ enabled phone, an iPhone®, and an iPad®.

The base transceiver station **124** may be any of a cellular wireless base station, for example a Code Division Multiple Access (CDMA), a Global System for Mobile Communications (GSM), a Universal Mobile Communications System (UMTS), and/or Long-term Evolution (LTE) cellular wireless base station; a Worldwide Interoperability for Microwave Access (WiMAX) base station; a WiFi access point; a femtocell; or other wireless access devices. While FIG. **1** depicts

only one base transceiver station **124**, in an embodiment a plurality of base transceiver stations **124** may be existent and in operation.

The network **106** promotes communication between the components of the system **100**. The network **106** may be any communication network including a public data network (PDN), a public switched telephone network (PSTN), a private network, a local area network (LAN), a wide area network (WAN), an intranet, the Internet and/or a combination of networks.

Authentication server **110** authenticates mobile device **140** to session server **120**. Authentication server **110** includes a token component **112** which generates a token which is transmitted to mobile device **140** to use to authenticate itself to a session. In an embodiment, token component **112** receives an indication of the location of mobile device **140**. Token component **112** may use the location information from the mobile device **140** to create a token.

Mobile device **140** sends a request for a token to authentication server **110**. The request may include location information about the mobile device **140**. Mobile device **140** receives the token from authentication server **110**. The token may be time and location limited. Additional details concerning time limited tokens may be found in U.S. patent application Ser. No. 13/042,015 to V. Cherukumudi, et al. filed Mar. 7, 2011 and entitled "Password Generation and Validation Method" which is incorporated herein by reference. Mobile device **140** may initiate an application level session with session server **120**. Examples of application level sessions may include logging into a bank's web site to check bank account information, checking e-mail through a web site, and performing work related activities on an employer's confidential web site. An application level session is a temporary interactive secure information exchange between collaborating application entities such as an application client and an application server during which the entities may transmit and receive requests and transmit and receive responses in the context of a previously completed authentication and authorization. An application level session is intended to preserve and protect access to and modification of secured information by authorized users and exclude unauthorized users.

An application level session should not be confused with other types of sessions occurring at other layers in an Open Systems Interconnection (OSI) model or in another layered communication stack model where a layer serves the layer above it and is served by the layer below it. For example, an application level session should not be confused with activities that occur at the physical layer, the data link layer, the network layer, the transport layer, the session layer, or the presentation layer. It will be understood that hereinafter references to a "session" mean an application level session as defined above. When communicating with the session server, the mobile device includes the token with each message transmitted. In an embodiment, the token may be communicated directly to the session server **120** which may then communicate with authentication server **110** to verify that the token is valid. In an embodiment, the token may be communicated directly to the authentication server **110** which may then provide an indication to the session server **120** of whether the token is valid and whether the session activity may be continued. If the token is valid, the session server **120** may perform session activities requested by the mobile device **140**. In an embodiment, the session server **120** may retrieve, store, or modify data in session data store **130**. For example, the data in session data store **130** may be account balance information for a bank account belonging to the user of mobile device **140**.

In an embodiment, the mobile device **140** transmits current location information along with the token to the authentication server **110**. The authentication server **110** determines whether the location for which the token was granted matches the current location information. If the current location of the mobile device **140** does not match the location information associated with the token, then the session is terminated. In an embodiment, the current location of the mobile device **140** matches the location associated with the token if the mobile device **140** is within an area **150** defined with reference to the location associated with the token. In an embodiment, the area **150** may be specified or defined as a specific or predefined radius extending from a point of a radio transceiver with which the location associated with the token corresponds. In an embodiment, the area **150** may be defined as within the specified building, such as a store location. In an embodiment, the area **150** may be specified as the area within which the mobile device **140** is able to communicate with a specified or predefined transceiver or radio source or one of a plurality of specified or predefined transceivers or radio sources.

In an embodiment, mobile device **140** may transmit session activity information, current location information, the token, and the session message to the authentication server **110** and/or session server **120**. In an embodiment, if sufficient activity on the mobile device **140** has occurred within a specified or predefined time prior to the receipt of the session message and token, then the session may be maintained even though the mobile device **140** may be outside of the location specified by the token. For example, if there has been continuing session activity while the mobile device **140** was moved from the location associated with the token to a new location, this activity may be used to infer that the mobile device **140** has not been stolen or otherwise compromised thereby minimizing the risk of unauthorized session activity. In an embodiment sufficient activity will maintain the session outside of a first area **150**, but only so long as the mobile device remains within a second area **160**. The second area **160** may be defined in a similar manner to that of first area **150**.

In an embodiment, lack of sufficient activity by the mobile device **140** on the session will cause the session to terminate at an earlier time than would otherwise be the case. This same concept may be expressed in terms of extending the life of the session if a sufficient amount of activity on the mobile device **140** is detected. In both cases, the session life span is different depending on the level of activity on the mobile device **140**. In an embodiment, the mobile device **140** may include a global session manager that monitors activity on several sessions. Activity on one session may provide the sufficient activity necessary to maintain or extend the session on the mobile device **140**.

Turning now to FIG. **2**, a block diagram of an embodiment of the token component **112** is provided. The token component **112** may comprise an encryption component **202** and may perform one or more steps for processing a plurality of inputs to generate a token **220**.

In an embodiment, the plurality of inputs comprises a time input **214***a*, a private data input **214***b*, and a public data input **214***c* which includes a location input **214***d*. The time input **214***a* may be provided by a clock **212** located on the authentication server **110**. The clock **212** may be a system clock. In an embodiment, the time input **214***a* is in DDDHHMM format where DDD is the day of the year, HH is the hour, and MM is the minute. Having the time input **214***a* in DDDHHMM format rather than some other longer time format helps to reduce the size of the unencrypted token **216**. However, the time input **214***a* could alternatively be in YYMMDDHHMM

format where YYMMDD is year, month, and day, HH is the hour, and MM is the minute or some other time format. The time input **214***a* could be a number of seconds elapsed in a predefined epoch, for example seconds elapsed since Jan. 1, 1970. The time input could be represented and/or processed in accordance with a different time keeping convention.

The time input **214***a* may be determined by rounding a current time to the nearest predefined time interval. For example, if the predefined time interval is selected to be 5 minutes and the current time is Jan. 17, 2011 at 9:32:23 am, the time input **214***a* in DDDHHMM format would be 0170930. Those of ordinary skill in the art will appreciate that the predefined time interval may be selected to be any interval of time. For instance, the predefined time interval may be 60 minutes, 30 minutes, 15 minutes, 5 minutes, 1 minute, or some other time interval. For the sake of simplicity, it may be beneficial to select a time interval that can be evenly divided into 60.

The time rounded to the nearest predefined time interval to determine the time input **214***a* may depend upon whether the token component **112** is generating a token **220** or validating a received token. For example, if the token component **112** is generating a token **220**, the time that may be rounded to the nearest predefined time interval may be the time that the mobile device **140** invoked the application program interface. In another example, if the token component **112** is validating a received token, the time that may be rounded to the nearest predefined time interval may be the time that the received token was received by the token component **112**.

The private data input **214***b* may be a secret key or phrase. In an embodiment, the private data input **214***b* is stored on the authentication server **110** in a data store or on some other server accessible to the token component **112**. The private data input **214***b* may be private in that it is accessible to the token component **112**, but not to the mobile device **140** and/or session server **120**. To help maintain security, the private data input **214***b* may be changed by an administrator or some other personnel regularly such as at some periodic time interval or irregularly.

The public data input **214***c* may be data that is known to a user of the mobile device **140**. The public data input **214***c* may include a location input **214***d* indicating the location of mobile device **140**. The public data input **214***c* may vary depending upon the context in which the token generation and validation system and methods disclosed herein are applied. For example, in a retail setting where authentication of an employee is sought, the public data input **214***c* may be a consumer ID, a user name, a store ID, a store location, and/or some other data know to the user of the mobile device **140**. In an embodiment, the store location may be determined from the store ID. To increase the strength of the generated token, two or more pieces of data can be included in the public data input **214***c*. The public data input **214***c* may be provided to the token component **112** from the mobile device **140** when the mobile device requests generation of a token **220** or by session server **120** when the session server **120** requests validation of a received token.

In an embodiment, an unencrypted token **216** may be formed from a plurality of inputs. For example, the unencrypted token **216** may be formed from the time input **214***a*, the private data input **214***b*, and the public data input **214***c*, including the location data **214***d*. In an embodiment, the unencrypted token **216** may be a string of characters.

The encryption component **202** may alter the unencrypted token **216** by applying a one-way hashing algorithm to the unencrypted token **216**. In an embodiment, applying a one-way hashing algorithm to the unencrypted token **216** produces a hashed string of characters that is not easily, if at all, able to be reversed back into the plurality of inputs used to create the unencrypted token **216**. For example, the encryption component **202** may apply a one-way hashing algorithm such as SHA-1, MD5, or another hashing algorithm. In some embodiments, the hashed string of characters that results from the encryption component **202** is the token **220**. Such an embodiment may be, for example, when the mobile device **140** communicates a token directly to the session server **120**. Other encryption techniques other than or in addition to hashing may also be utilized in generating the token **220**.

Turning now to FIG. **3**, a block diagram of an embodiment of the mobile device **140** is provided. Mobile device **140** may include token **1 302**, token **2 304**, token **3 306**, a location determination component **308**, and a global session manager **310**. The location determination component **308** may determine the location of the mobile device **140** and provide that information to the authentication server **110**. In an embodiment, the location determination component **308** may comprise a Global Positioning System (GPS) component to determine the location of the mobile device **140** based on GPS coordinates. In an embodiment, the location determination component **308** determines the location of the mobile device **140** based on signal strength from one or more radio transceivers. In an embodiment, the location determination component **308** determines the location of the mobile device **140** based on the identity of a transceiver with which the mobile device **140** is in communication.

Global session manager **310** may monitor activity on multiple sessions associated with tokens **302**, **304**, **306**. Global Session Manager **310** may be acquired from a source that is trusted by the originators of the tokens **302**, **304**, **306**. The sessions associated with each of tokens **302**, **304**, **306** may be time limited and be set to expire unless a sufficient level of activity is maintained within a specified period of time on the mobile device **140**. However, since the global session manager **310** may be trusted by the sessions associated with tokens **302**, **304**, **306**, rather than prematurely ending one session due to lack of activity on the mobile device **140**, the session may be maintained if sufficient activity occurs on one of the other sessions associated with one of the other tokens **302**, **304**, **306**. During a session, when the mobile device **140** transmits a session message to the authentication server **110** or session server **120**, the mobile device **140** may also transmit the corresponding token, the current location of the mobile device **140**, and the session activity as determined by the global session manager **310**.

Turning to FIG. **4**, a flowchart of a method **400** for generating a token is depicted in accordance with an embodiment of the present disclosure. Method **400** begins at block **410** where the authentication server **110** receives a plurality of inputs from the mobile device **140** where the inputs include a device location and a first time. At block **412**, the authentication server **110** generates a string of characters from at least some of the plurality of inputs, wherein the inputs include at least the mobile device location and the first time. At block **414**, the authentication server **110** hashes the string of characters. At block **416**, the authentication server **110** may encode the hashed string of characters, after which the method **400** may end.

Turning to FIG. **5**, a flowchart of a method **500** for validating a token is depicted in accordance with an embodiment of the present disclosure. Method **500** begins at block **510** where the authentication server **110** receives a current location of the mobile device **140**, an activity level of the mobile device **140**, and a token from the mobile device **140** or from the session server **120**. At block **512**, the authentication server **110** deter-

mines whether the token is valid. If the token is not valid, the method **500** proceeds to block **524** where the session is ended at which point method **500** may end. If the authentication server **110** determines that the token is valid at block **512**, then the method **500** proceeds to block **514** where the authentication server **110** determines whether the current location matches a location for which the token is valid. If, at block **514**, the authentication server **110** determines that the current location does not match the location for which the token is valid, then the method **500** proceeds to block **516** or alternatively, the method **500** may proceed to block **524** where the session is ended and the method **500** may end. At block **516**, the authentication server **110** determines whether there has been sufficient continuing activity on the session (or alternatively on the mobile device **140** generally) to warrant allowing the session to continue although the mobile device **140** is outside the location where the token is valid. If, at block **516**, sufficient continuing activity has not been maintained on the session or the mobile device **140**, then method **500** proceeds to block **524** where the session is ended at which point the method **500** may end.

If, at block **514**, the authentication server **110** determines that the current location matches the location for which the token is valid or, at block **516**, the authentication server **110** determines that there has been sufficient continuing activity to warrant maintaining the session, the method **500** proceeds to block **518**. At block **518**, the authentication server **110** determines whether the predefined time limit for which the token is valid has expired. If, at block **518**, the authentication server **110** determines that the predefined time limit has not expired, then the method **500** proceeds to block **522** where the token is authenticated allowing the session to continue. Once the token has been authenticated at block **522**, the method **500** may end.

If, at block **518**, the authentication server **110** determines that the time limit has expired, the method **500** proceeds to block **520**. Alternatively, the method **500** may proceed to block **524** if the authentication server **110** determines that the time limit has expired. At block **520**, the authentication server **110** determines whether there has been sufficient activity within a predetermined time period to allow the session to be extended. If, at block **520**, the authentication server **110** determines that there has been insufficient activity, then the method **500** proceeds to block **524** after which method **500** may end. If, at block **520**, the authentication server **110** determines that there has been sufficient activity, then the method **500** may proceed to block **522** where the token is authenticated. Once the token has been authenticated at block **522**, the method **500** may end. As discussed above, the activity level may be based solely on the activity level in the session corresponding to the token to be authenticated. However, in an embodiment, also discussed above, the activity level may be based on activity on other sessions not corresponding to the token to be authenticated. Those skilled in the art will recognize that the decision diamonds illustrated in FIG. **5** may be reordered in several ways to implement the checks described therein. For example, in an embodiment, a time limit associated with the token may be checked before the current location is checked against a location associated with the token. In an embodiment, the sufficient continuing activity criteria may be checked before either the current location criteria or the time limit criteria is checked.

FIG. **6** shows a wireless communications system including the mobile device **600**. FIG. **6** depicts the mobile device **600**, which is operable for implementing aspects of the present disclosure, but the present disclosure should not be limited to these implementations. Though illustrated as a mobile phone, the mobile device **600** may take various forms including a wireless handset, a pager, a personal digital assistant (PDA), a gaming device, or a media player. The mobile device **600** includes a display **602** and a touch-sensitive surface and/or keys **604** for input by a user. The mobile device **600** may present options for the user to select, controls for the user to actuate, and/or cursors or other indicators for the user to direct. The mobile device **600** may further accept data entry from the user, including numbers to dial or various parameter values for configuring the operation of the handset. The mobile device **600** may further execute one or more software or firmware applications in response to user commands. These applications may configure the mobile device **600** to perform various customized functions in response to user interaction. Additionally, the mobile device **600** may be programmed and/or configured over-the-air, for example from a wireless base station, a wireless access point, or a peer mobile device **600**. The mobile device **600** may execute a web browser application which enables the display **602** to show a web page. The web page may be obtained via wireless communications with a base transceiver station, a wireless network access node, a peer mobile device **600** or any other wireless communication network or system.

FIG. **7** shows a block diagram of the mobile device **600**. While a variety of known components of handsets are depicted, in an embodiment a subset of the listed components and/or additional components not listed may be included in the mobile device **600**. The mobile device **600** includes a digital signal processor (DSP) **702** and a memory **704**. As shown, the mobile device **600** may further include an antenna and front end unit **706**, a radio frequency (RF) transceiver **708**, a baseband processing unit **710**, an input/output interface **718**, a removable memory card **720**, a universal serial bus (USB) port **722**, an infrared port **724**, a vibrator **726**, a keypad **728**, a touch screen liquid crystal display (LCD) with a touch sensitive surface **730**, a touch screen/LCD controller **732**, a camera **734**, a camera controller **736**, a global positioning system (GPS) receiver **738**, and a sensor **740**. In an embodiment, the mobile device **600** may include another kind of display that does not provide a touch sensitive screen. In an embodiment, the DSP **702** may communicate directly with the memory **704** without passing through the input/output interface **718**. Additionally, in an embodiment, the mobile device **600** may comprise other peripheral devices that provide other functionality.

The DSP **702** or some other form of controller or central processing unit operates to control the various components of the mobile device **600** in accordance with embedded software or firmware stored in memory **704** or stored in memory contained within the DSP **702** itself. In addition to the embedded software or firmware, the DSP **702** may execute other applications stored in the memory **704** or made available via information carrier media such as portable data storage media like the removable memory card **720** or via wired or wireless network communications. The application software may comprise a compiled set of machine-readable instructions that configure the DSP **702** to provide the desired functionality, or the application software may be high-level software instructions to be processed by an interpreter or compiler to indirectly configure the DSP **702**.

The DSP **702** may communicate with a wireless network via the analog baseband processing unit **710**. In some embodiments, the communication may provide Internet connectivity, enabling a user to gain access to content on the Internet and to send and receive e-mail or text messages. The input/output interface **718** interconnects the DSP **702** and various memories and interfaces. The memory **704** and the

removable memory card **720** may provide software and data to configure the operation of the DSP **702**. Among the interfaces may be the USB port **722** and the infrared port **724**. The USB port **722** may enable the mobile device **600** to function as a peripheral device to exchange information with a personal computer or other computer system. The infrared port **724** and other optional ports such as a Bluetooth® interface or an IEEE 702.11 compliant wireless interface may enable the mobile device **600** to communicate wirelessly with other nearby handsets and/or wireless base stations.

The keypad **728** couples to the DSP **702** via the interface **718** to provide one mechanism for the user to make selections, enter information, and otherwise provide input to the mobile device **600**. Another input mechanism may be the touch screen LCD **730**, which may also display text and/or graphics to the user. The touch screen LCD controller **732** couples the DSP **702** to the touch screen LCD **730**. The GPS receiver **738** is coupled to the DSP **702** to decode global positioning system signals, thereby enabling the mobile device **600** to determine its position.

Sensor **740** couples to the DSP **702** via the interface **718** to provide a mechanism to determine movement and/or relative orientation of the mobile device **600**. The sensor **740** may provide information to DSP **702** indicating the orientation that the mobile device **600** is being held (e.g., face up, face down, face perpendicular to the ground). Sensor **740** may also provide information indicating whether the mobile device **600** is being moved (e.g., right to left, up to down) and indicate sudden accelerations and/or decelerations. Sudden decelerations may indicate that the mobile device **600** has been dropped. Sensor **740** may include an accelerometer to measure various motions and orientations of the mobile device **600**. Measurements from sensor **740** may be provided to DSP **702** which may record the measurement and a time stamp in a log file stored, for example, in memory **704**.

In an embodiment, sensor **740** may include other sensors, such as, for example, a temperature sensor and/or a current meter for measuring current flow from the mobile device's **600** battery. The temperature sensor may detect the temperature of the mobile device **600** or various components of the mobile device **600** to indicate whether a component (e.g., an RF circuit) may be over heating. Additionally, in an embodiment, the mobile device **600** may comprise other sensors that provide other functionality.

FIG. **8**A illustrates a software environment **802** that may be implemented by the DSP **702**. The DSP **702** executes operating system software **804** that provides a platform from which the rest of the software operates. The operating system software **804** may provide a variety of drivers for the handset hardware with standardized interfaces that are accessible to application software. The operating system software **804** may be coupled to and interact with application management services (AMS) **806** that transfer control between applications running on the mobile device **600**. Also shown in FIG. **8**A are a web browser application **808**, a media player application **810**, JAVA applets **812**, and a global session manager (GSM) **814**. The web browser application **808** may be executed by the mobile device **600** to browse content and/or the Internet, for example when the mobile device **600** is coupled to a network via a wireless link. The web browser application **808** may permit a user to enter information into forms and select links to retrieve and view web pages. The media player application **810** may be executed by the mobile device **600** to play audio or audiovisual media. The JAVA applets **812** may be executed by the mobile device **600** to provide a variety of functionality including games, utilities, and other functionality. The GSM **814** may be executed by the mobile device **600** to manage one or more sessions on the mobile device **600**. The GSM may monitor session activity on multiple sessions and provide the session activity to other sessions so that a session does not prematurely end due to lack of activity on that particular session when there is still sufficient activity on another session to warrant keeping the particular session alive.

FIG. **8**B illustrates an alternative software environment **820** that may be implemented by the DSP **702**. The DSP **702** executes operating system software **828** and an execution runtime **830**. The DSP **702** executes applications **822** that may execute in the execution runtime **830** and may rely upon services provided by the application framework **824**. Applications **822** and the application framework **824** may rely upon functionality provided via the libraries **826**.

FIG. **9** illustrates a computer system **980** suitable for implementing one or more embodiments disclosed herein. The computer system **980** includes a processor **982** (which may be referred to as a central processor unit or CPU) that is in communication with memory devices including secondary storage **984**, read only memory (ROM) **986**, random access memory (RAM) **988**, input/output (I/O) devices **990**, and network connectivity devices **992**. The processor **982** may be implemented as one or more CPU chips.

It is understood that by programming and/or loading executable instructions onto the computer system **980**, at least one of the CPU **982**, the RAM **988**, and the ROM **986** are changed, transforming the computer system **980** in part into a particular machine or apparatus having the novel functionality taught by the present disclosure. It is fundamental to the electrical engineering and software engineering arts that functionality that can be implemented by loading executable software into a computer can be converted to a hardware implementation by well known design rules. Decisions between implementing a concept in software versus hardware typically hinge on considerations of stability of the design and numbers of units to be produced rather than any issues involved in translating from the software domain to the hardware domain. Generally, a design that is still subject to frequent change may be preferred to be implemented in software, because re-spinning a hardware implementation is more expensive than re-spinning a software design. Generally, a design that is stable that will be produced in large volume may be preferred to be implemented in hardware, for example in an application specific integrated circuit (ASIC), because for large production runs the hardware implementation may be less expensive than the software implementation. Often a design may be developed and tested in a software form and later transformed, by well known design rules, to an equivalent hardware implementation in an application specific integrated circuit that hardwires the instructions of the software. In the same manner as a machine controlled by a new ASIC is a particular machine or apparatus, likewise a computer that has been programmed and/or loaded with executable instructions may be viewed as a particular machine or apparatus.

The secondary storage **984** is typically comprised of one or more disk drives or tape drives and is used for non-volatile storage of data and as an over-flow data storage device if RAM **988** is not large enough to hold all working data. Secondary storage **984** may be used to store programs which are loaded into RAM **988** when such programs are selected for execution. The ROM **986** is used to store instructions and perhaps data which are read during program execution. ROM **986** is a non-volatile memory device which typically has a small memory capacity relative to the larger memory capacity of secondary storage **984**. The RAM **988** is used to store volatile data and perhaps to store instructions. Access to both

ROM **986** and RAM **988** is typically faster than to secondary storage **984**. The secondary storage **984**, the RAM **988**, and/or the ROM **986** may be referred to in some contexts as computer readable storage media and/or non-transitory computer readable media.

I/O devices **990** may include printers, video monitors, liquid crystal displays (LCDs), touch screen displays, keyboards, keypads, switches, dials, mice, track balls, voice recognizers, card readers, paper tape readers, or other well-known input devices.

The network connectivity devices **992** may take the form of modems, modem banks, Ethernet cards, universal serial bus (USB) interface cards, serial interfaces, token ring cards, fiber distributed data interface (FDDI) cards, wireless local area network (WLAN) cards, radio transceiver cards such as code division multiple access (CDMA), global system for mobile communications (GSM), long-term evolution (LTE), worldwide interoperability for microwave access (WiMAX), and/or other air interface protocol radio transceiver cards, and other well-known network devices. These network connectivity devices **992** may enable the processor **982** to communicate with the Internet or one or more intranets. With such a network connection, it is contemplated that the processor **982** might receive information from the network, or might output information to the network in the course of performing the above-described method steps. Such information, which is often represented as a sequence of instructions to be executed using processor **982**, may be received from and outputted to the network, for example, in the form of a computer data signal embodied in a carrier wave.

Such information, which may include data or instructions to be executed using processor **982** for example, may be received from and outputted to the network, for example, in the form of a computer data baseband signal or signal embodied in a carrier wave. The baseband signal or signal embedded in the carrier wave, or other types of signals currently used or hereafter developed, may be generated according to several methods well known to one skilled in the art. The baseband signal and/or signal embedded in the carrier wave may be referred to in some contexts as a transitory signal.

The processor **982** executes instructions, codes, computer programs, scripts which it accesses from hard disk, floppy disk, optical disk (these various disk based systems may all be considered secondary storage **984**), ROM **986**, RAM **988**, or the network connectivity devices **992**. While only one processor **982** is shown, multiple processors may be present. Thus, while instructions may be discussed as executed by a processor, the instructions may be executed simultaneously, serially, or otherwise executed by one or multiple processors. Instructions, codes, computer programs, scripts, and/or data that may be accessed from the secondary storage **984**, for example, hard drives, floppy disks, optical disks, and/or other device, the ROM **986**, and/or the RAM **988** may be referred to in some contexts as non-transitory instructions and/or non-transitory information.

In an embodiment, the computer system **980** may comprise two or more computers in communication with each other that collaborate to perform a task. For example, but not by way of limitation, an application may be partitioned in such a way as to permit concurrent and/or parallel processing of the instructions of the application. Alternatively, the data processed by the application may be partitioned in such a way as to permit concurrent and/or parallel processing of different portions of a data set by the two or more computers. In an embodiment, virtualization software may be employed by the computer system **980** to provide the functionality of a number of servers that is not directly bound to the number of computers in the computer system **980**. For example, virtualization software may provide twenty virtual servers on four physical computers. In an embodiment, the functionality disclosed above may be provided by executing the application and/or applications in a cloud computing environment. Cloud computing may comprise providing computing services via a network connection using dynamically scalable computing resources. Cloud computing may be supported, at least in part, by virtualization software. A cloud computing environment may be established by an enterprise and/or may be hired on an as-needed basis from a third party provider. Some cloud computing environments may comprise cloud computing resources owned and operated by the enterprise as well as cloud computing resources hired and/or leased from a third party provider.

In an embodiment, some or all of the functionality disclosed above may be provided as a computer program product. The computer program product may comprise one or more computer readable storage medium having computer usable program code embodied therein to implement the functionality disclosed above. The computer program product may comprise data structures, executable instructions, and other computer usable program code. The computer program product may be embodied in removable computer storage media and/or non-removable computer storage media. The removable computer readable storage medium may comprise, without limitation, a paper tape, a magnetic tape, magnetic disk, an optical disk, a solid state memory chip, for example analog magnetic tape, compact disk read only memory (CD-ROM) disks, floppy disks, jump drives, digital cards, multimedia cards, and others. The computer program product may be suitable for loading, by the computer system **980**, at least portions of the contents of the computer program product to the secondary storage **984**, to the ROM **986**, to the RAM **988**, and/or to other non-volatile memory and volatile memory of the computer system **980**. The processor **982** may process the executable instructions and/or data structures in part by directly accessing the computer program product, for example by reading from a CD-ROM disk inserted into a disk drive peripheral of the computer system **980**. Alternatively, the processor **982** may process the executable instructions and/or data structures by remotely accessing the computer program product, for example by downloading the executable instructions and/or data structures from a remote server through the network connectivity devices **992**. The computer program product may comprise instructions that promote the loading and/or copying of data, data structures, files, and/or executable instructions to the secondary storage **984**, to the ROM **986**, to the RAM **988**, and/or to other non-volatile memory and volatile memory of the computer system **980**.

In some contexts, the secondary storage **984**, the ROM **986**, and the RAM **988** may be referred to as a non-transitory computer readable medium or a computer readable storage media. A dynamic RAM embodiment of the RAM **988**, likewise, may be referred to as a non-transitory computer readable medium in that while the dynamic RAM receives electrical power and is operated in accordance with its design, for example during a period of time during which the computer **980** is turned on and operational, the dynamic RAM stores information that is written to it. Similarly, the processor **982** may comprise an internal RAM, an internal ROM, a cache memory, and/or other internal non-transitory storage blocks, sections, or components that may be referred to in some contexts as non-transitory computer readable media or computer readable storage media.

While several embodiments have been provided in the present disclosure, it should be understood that the disclosed

systems and methods may be embodied in many other specific forms without departing from the spirit or scope of the present disclosure. The present examples are to be considered as illustrative and not restrictive, and the intention is not to be limited to the details given herein. For example, the various elements or components may be combined or integrated in another system or certain features may be omitted or not implemented.

Also, techniques, systems, subsystems, and methods described and illustrated in the various embodiments as discrete or separate may be combined or integrated with other systems, modules, techniques, or methods without departing from the scope of the present disclosure. Other items shown or discussed as directly coupled or communicating with each other may be indirectly coupled or communicating through some interface, device, or intermediate component, whether electrically, mechanically, or otherwise. Other examples of changes, substitutions, and alterations are ascertainable by one skilled in the art and could be made without departing from the spirit and scope disclosed herein.

What is claimed is:

1. A location aware session token generation and validation system, comprising:

a server system comprising at least one processor;

at least one non-transitory memory coupled to the at least one processor; and

a token component stored in the at least one non-transitory memory that, upon execution by the at least one processor of the server system, configures the server system to:

receive a request to initiate an application level session from a mobile device comprising a global session management component stored in non-transitory memory of the mobile device, wherein the request includes an identification of the mobile device and a location of the mobile device within a predefined area of a communication network,

generate a token that initiates the application level session based on the request, wherein the token is time limited to a specified period of time and location limited to the predefined area such that the application level session is designated to expire based on at least one of the end of the specified period of time or the mobile device moving outside of the predefined area,

send the token to the mobile device via the communication network, wherein the mobile device comprises a plurality of tokens that each correspond to a respective one of a plurality of application level sessions, wherein each application level session includes an interactive secure information exchange between an application server and an application via a radio transceiver of the mobile device based on a completed authentication and authorization for the application that is stored in a non-transitory memory of the mobile device,

receive an application level session message from the mobile device using the global session management component, wherein the application level session message includes a requested application level session action associated with the application level session, a current location of the mobile device, and the token for the application level session,

determine, by analysis of the token, that the current location does not match the location associated with the token due to the mobile device moving outside of the predefined area and that a level of activity on the mobile device meets or exceeds a pre-specified level of activity,

responsive to the determination, extend the application level session associated with the token despite the current location of the mobile device being outside of the predefined area, and

perform the requested application level session action based on the extended application level session.

2. The location aware session token generation and validation system of claim **1**, wherein determination that the level of activity on the mobile device meets or exceeds the pre-specified level of activity is responsive to the determination that the current location does not match the location.

3. The location aware session token generation and validation system of claim **1**, wherein the level of activity on the mobile device that meets or exceeds the pre-specified level of activity is associated with at least one of the plurality of application level sessions.

4. The location aware session token generation and validation system of claim **1**, wherein the current location is within a predefined radius from a point corresponding to the determined location associated with the token.

5. The location aware session token generation and validation system of claim **1**, wherein the location associated with the token is within the predefined area based on proximity to a predefined radio source of the communication network.

6. The location aware session token generation and validation system of claim **5**, wherein the predefined radio source comprises one of a particular local network, a particular WiFi network, and a particular base station tower.

7. The location aware session token generation and validation system of claim **1**, wherein the requested session action comprises one of manipulating data on a data store, retrieving data from the data store and sending the data to the mobile device, or receiving data from the mobile device and storing the data on the data store.

8. A cross application session management system for a mobile device, comprising:

a mobile device comprising:

a radio transceiver that couples to a communication network,

at least one processor,

at least one non-transitory memory coupled to the at least one processor,

a plurality of tokens stored in the at least one non-transitory memory, wherein each of the plurality of tokens corresponds to a respective one of a plurality of application level sessions, and each of the plurality of tokens is associated with a location within a predefined area of the communication network, and

a global session management component stored in the at least one non-transitory memory that, upon execution by the at least one processor, configures the mobile device to:

monitor activity on the plurality of application level sessions, wherein each application level session includes an interactive secure information exchange between an application server and an application via the radio transceiver based on a completed authentication and authorization for the application that is stored in the at least one non-transitory memory of the mobile device,

determine that activity on at least one of the plurality of application level sessions meets or exceeds a pre-specified level of activity, and

based on the determination, maintain the application level session life for at least another application level session of the plurality of application level sessions by sending: an application level session

message reporting the activity of the at least one of the plurality of application level sessions that meets or exceeds the pre-specified level of activity, a token corresponding to the another application level session, and a current location of the mobile device that is outside of the predefined area associated with the token, wherein the application level session is extended despite the current location of the mobile device being outside of the redefined area.

9. The system of claim **8**, wherein the token is designated to end the another application level session responsive to the current location of the mobile device not matching the location associated with the token.

10. The system of claim **9**, wherein the another application level session corresponding to the token that includes the location component is extended when the global session management component determines a specified level of activity on one of the plurality of application level sessions during movement of the mobile device.

11. The system of claim **10**, wherein the mobile device comprises at least one of a mobile telephone, a tablet computer, or a laptop computer.

12. A method for session management for a mobile device, comprising:

receiving, at an authenticating server executing at least one processor, a request for a token to authenticate an application level session with a communication network of a service provider, wherein the request includes an identification of the mobile device and a location of the mobile device within a predefined area of the communication network;

generating, by the authenticating server executing a token component, a token that initiates the application level session, wherein the token is time limited and location limited to a predefined area associated with the token at the time of generation;

sending, from the authenticating server, the token to the mobile device;

receiving, at the authenticating server, a session message for the application level session from the mobile device, wherein the session message includes a requested session action for the application level session, a current location of the mobile device, an activity level on the mobile device, and the token for the application level session, wherein the application level session includes an interactive secure information exchange between an application server and an application via a radio transceiver of the mobile device based on a completed authentication and authorization for the application that is stored a non-transitory memory of the mobile device;

determining, by the authentication server analyzing the token, that the current location does not match the location associated with the token due to the mobile device moving outside of the predefined area and that the activity level at least meets a pre-specified level of activity;

responsive to the determination, extending, by the authenticating server, the application level session associated with the token despite the current location of the mobile device being outside of the predefined area; and

performing the requested session action based on extending the application level session.

13. The method of claim **12**, wherein extending the application level session comprises extending the predefined period of time associated with expiration of the application level session.

14. The method of claim **12**, further comprising ending the application level session responsive to expiration of a predefined period of time associated with the token and a level of activity below the pre-specified level for all of a plurality of application level sessions associated with the mobile device.

15. The method of claim **12**, further comprising:

ending the application level session responsive to the current location not matching the location of the token and the activity level being less than the pre-specified level of activity.

16. The method of claim **12**, wherein the requested session action comprises at least one of manipulating data on a data store, retrieving data from the data store and sending the data to the mobile device, or receiving data from the mobile device and storing the data on the data store.

17. The method of claim **12**, wherein the activity level is the activity level corresponding to a different application level session.

18. The method of claim **12**, wherein the current location does not match the location when the current location is outside of the predefined area.

19. The method of claim **12**, wherein the mobile device comprises at least one of a mobile telephone, a tablet computer, or laptop computer.

20. The method of claim **12**, wherein the current location of the mobile device is based on at least one of global positioning system coordinates or triangulation within the communication network.

* * * * *