US 20140189840A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2014/0189840 A1**

(43) **Pub. Date: Jul. 3, 2014**

METKE et al.

(54) **METHOD AND APPARATUS FOR SINGLE SIGN-ON COLLABORATION AMONG MOBILE DEVICES**

(71) Applicant: **MOTOROLA SOLUTIONS, INC.**, Schaumburg, IL (US)

(72) Inventors: **ANTHONY R. METKE**, Naperville, IL (US); **Katrin Reitsma**, Chicago, IL (US); **Adam C. Lewis**, Buffalo Grove, IL (US); **George Popovich**, Palatine, IL (US); **Steven D. Upp**, Bartlett, IL (US)

(73) Assignee: **MOTOROLA SOLUTIONS, INC.**, Schaumburg, IL (US)

(21) Appl. No.: **13/728,422**

(22) Filed: **Dec. 27, 2012**

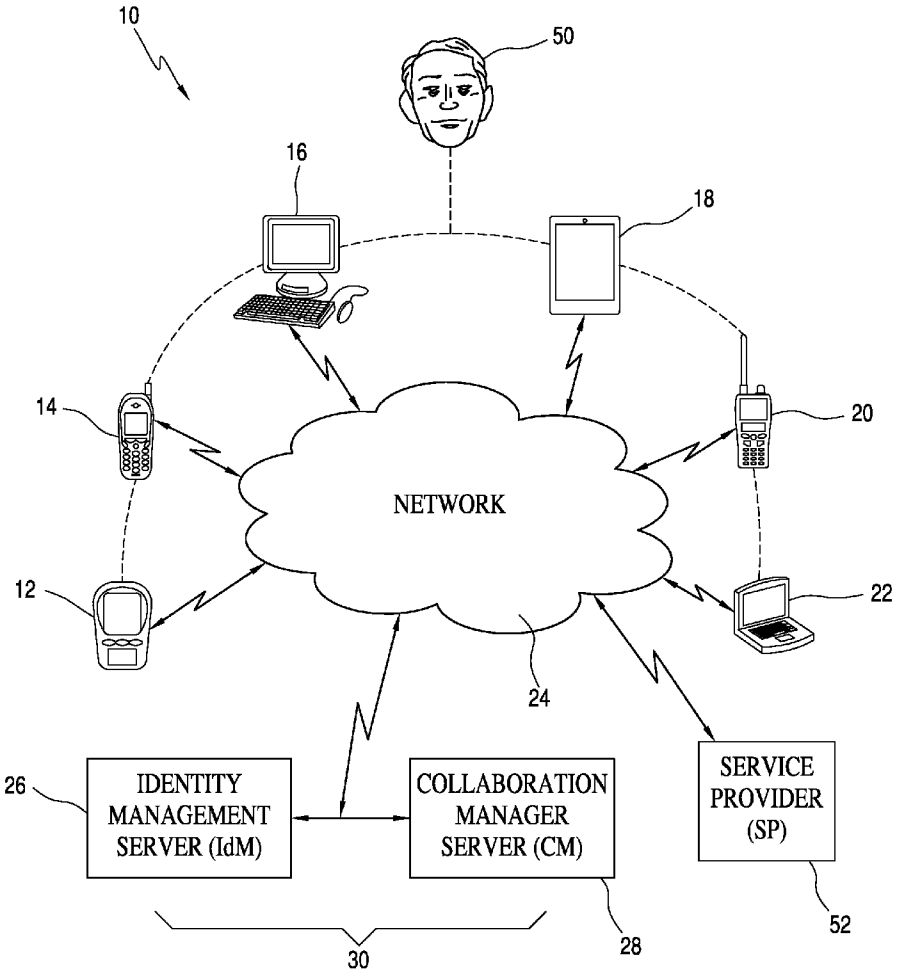
Publication Classification

(51) **Int. Cl.**
H04W 12/06 (2006.01)

(52) **U.S. Cl.**
CPC *H04W 12/06* (2013.01)
USPC **726/9**

(57) **ABSTRACT**

A system for, and method of, single sign-on collaboration among a plurality of mobile devices, includes a server for issuing a first identity token to subsequently authenticate a user of a first of the mobile devices to a service provider, and for generating and sending a collaboration credential to the first device based on the first identity token or user authentication. The first device sends the collaboration credential generated by the server to a second device paired with the first device. The server also issues a second identity token to subsequently authenticate to the service provider the user of the second device based on the collaboration credential received from the first device, to support single sign-on collaboration for the user across the plurality of mobile devices.



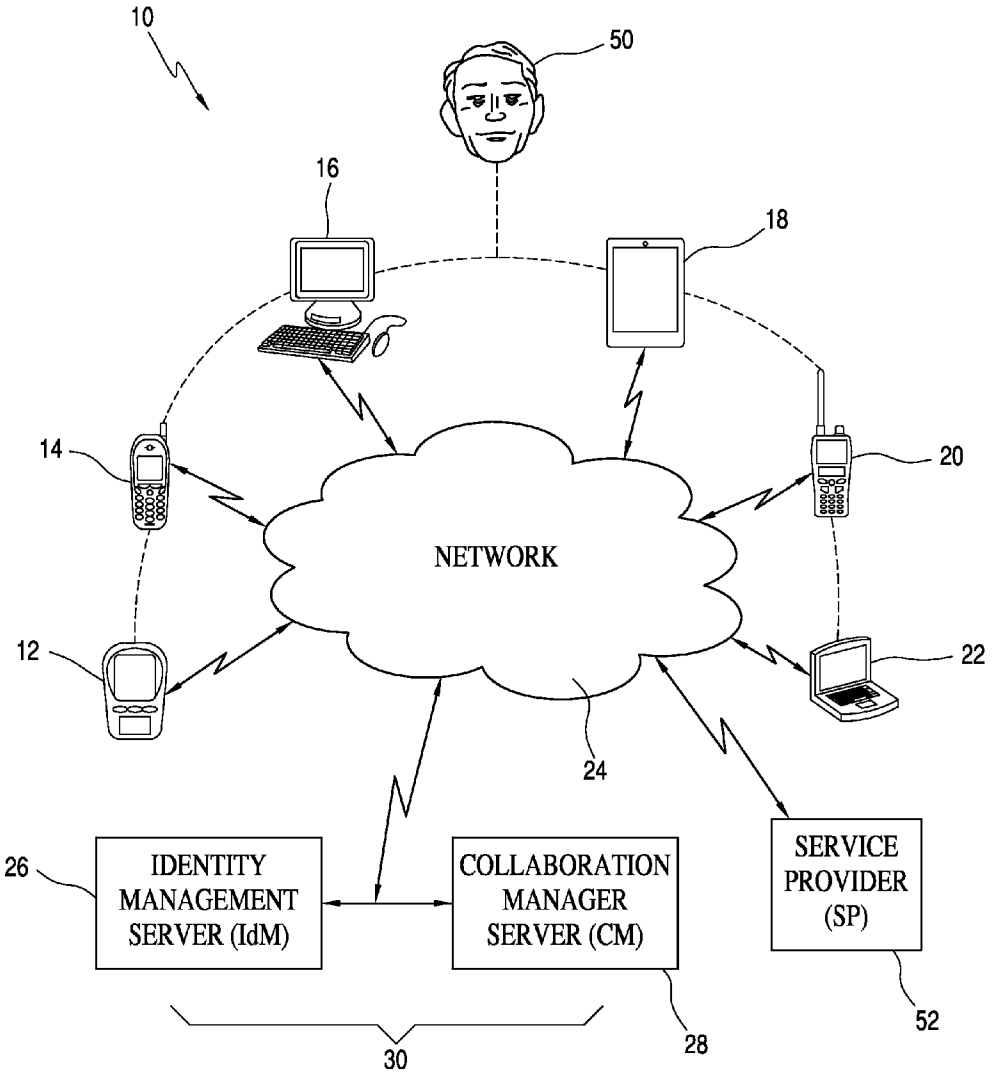

10
50
16
18
14
20
NETWORK
12
22
24
26
IDENTITY MANAGEMENT SERVER (IdM)
COLLABORATION MANAGER SERVER (CM)
SERVICE PROVIDER (SP)
52
28
30

FIG. 1

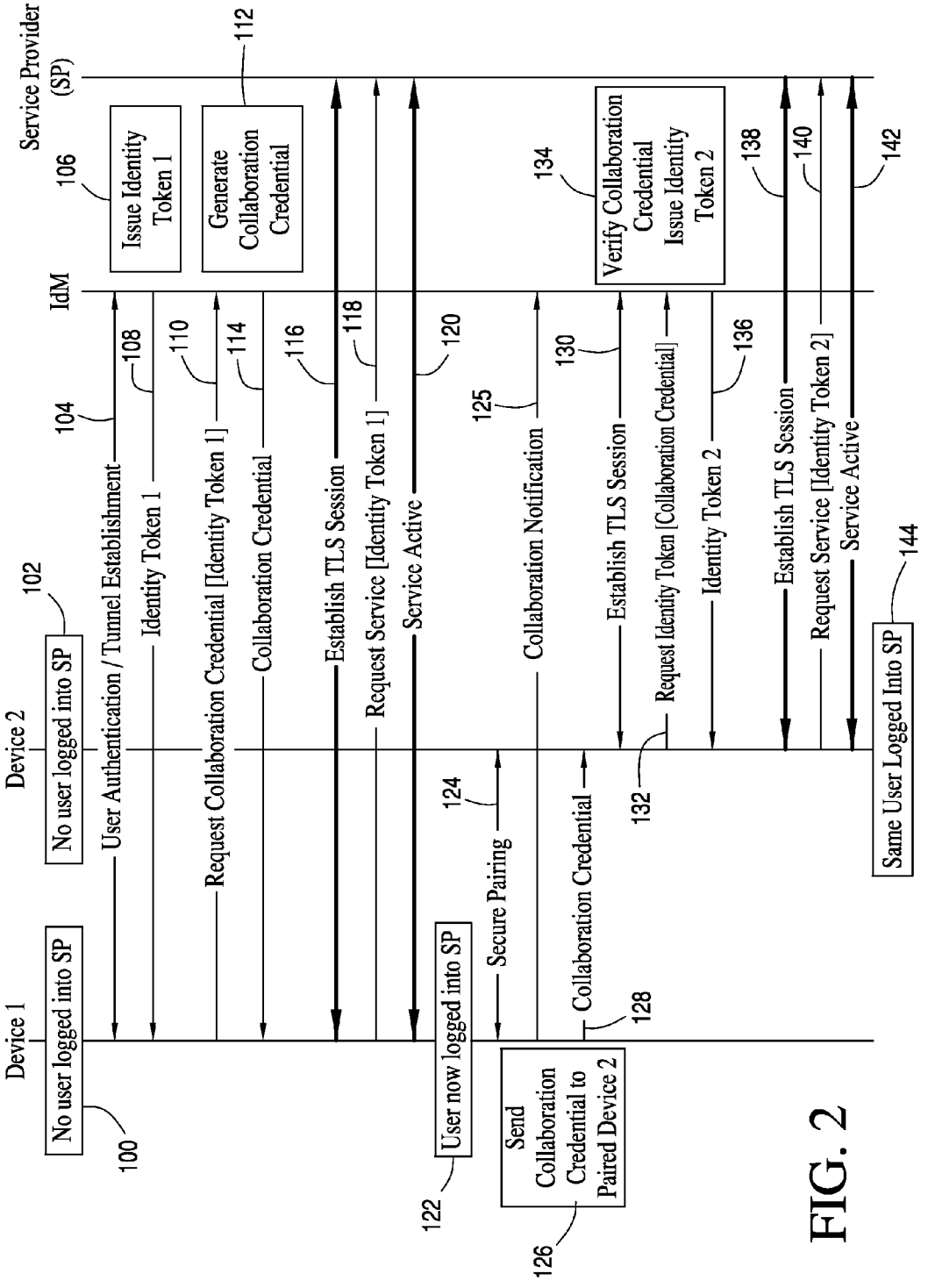

Device 1
Device 2
IdM
Service Provider (SP)
No user logged into SP
100
No user logged into SP
102
User Authentication / Tunnel Establishment
104
Issue Identity Token 1
106
Identity Token 1
108
Generate Collaboration Credential
112
Request Collaboration Credential [Identity Token 1]
110
Collaboration Credential
114
Establish TLS Session
116
Request Service [Identity Token 1]
118
Service Active
120
User now logged into SP
122
Secure Pairing
124
Collaboration Notification
125
Send Collaboration Credential to Paired Device 2
126
Collaboration Credential
128
Verify Collaboration Credential Issue Identity Token 2
134
Establish TLS Session
130
Request Identity Token [Collaboration Credential]
132
Identity Token 2
136
Establish TLS Session
138
Request Service [Identity Token 2]
140
Service Active
142
Same User Logged Into SP
144

FIG. 2

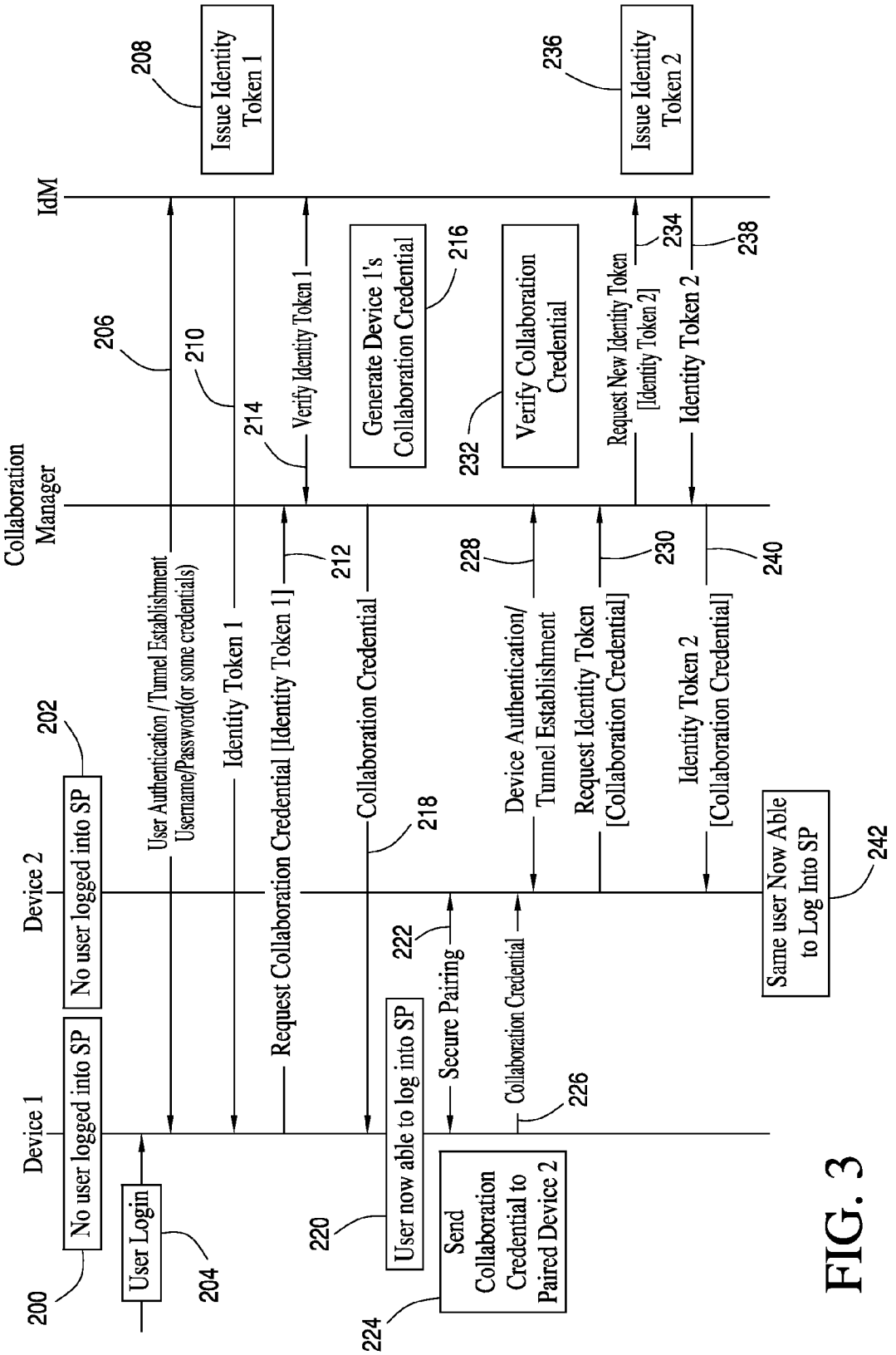

Device 1
Device 2
Collaboration Manager
IdM
No user logged into SP
No user logged into SP
User Login
User now able to log into SP
Send Collaboration Credential to Paired Device 2
Same user Now Able to Log Into SP
User Authentication / Tunnel Establishment
Username/Password(or some credentials)
Identity Token 1
Request Collaboration Credential [Identity Token 1]
Collaboration Credential
Secure Pairing
Collaboration Credential
Device Authentication/ Tunnel Establishment
Request Identity Token [Collaboration Credential]
Identity Token 2 [Collaboration Credential]
Issue Identity Token 1
Verify Identity Token 1
Generate Device 1's Collaboration Credential
Verify Collaboration Credential
Request New Identity Token [Identity Token 2]
Identity Token 2
Issue Identity Token 2
200
202
204
206
208
210
212
214
216
218
220
222
224
226
228
230
232
234
236
238
240
242

FIG. 3

METHOD AND APPARATUS FOR SINGLE SIGN-ON COLLABORATION AMONG MOBILE DEVICES

REFERENCE TO RELATED APPLICATIONS

[0001] The present application is related to U.S. patent application Ser. No. _____, attorney docket no. CM15507, entitled "Method of and System for Authenticating and Operating Personal Communication Devices over Public Safety Networks"; U.S. patent application Ser. No. _____, attorney docket no. CM15513, entitled "Method and Apparatus for Single Sign-On Collaboration Among Mobile Devices"; U.S. patent application Ser. No. _____, attorney docket no. CM15568, entitled "Method and Apparatus for Ensuring Collaboration Between a Narrowband Device and a Broadband Device"; U.S. patent application Ser. No. _____, attorney docket no. CM15610, entitled "System and Method for Scoping a User Identity Assertion to Collaborative Devices"; and U.S. patent application Ser. No. _____, attorney docket no. CM15805, entitled "Apparatus for and Method of Multi-Factor Authentication Among Collaborating Mobile Devices"; which applications are commonly owned and filed on the same date as this application and the contents of which applications are incorporated herein in their entirety by reference thereto.

FIELD OF THE DISCLOSURE

[0002] The present disclosure relates generally to a system for, and a method of, single sign-on (SSO) collaboration among a plurality of mobile devices.

BACKGROUND

[0003] Single sign-on (SSO) technology is a session/user authentication process that permits an on-line user to enter identity information, for example, a user name and a password, in response to prompts in order to access multiple applications, e.g., email, banking services, shopping services, etc., at various web sites or internet domains hosted by a service provider, on a single mobile device. The SSO process authenticates the user for all the applications that he or she has been given rights to, and eliminates further prompts when the user switches applications during a particular on-line session. Security Assertion Markup Language (SAML) and Web Authorization Protocol (OAuth) are examples of open standards for exchanging authentication and authorization data between such multiple applications on a single mobile device.

[0004] As advantageous as the known SSO processes have been, they do not support SSO when a user of one mobile device changes or switches to another mobile device. By way of example, a user may be checking his or her email on a personal digital assistant or a smartphone, and then, for whatever reason, may subsequently wish to check his or her email, or even run a different application, on his or her laptop computer or a desktop computer. Thereafter, the user may wish to check his or her email, or even run a different application, on his or her tablet. The user may, in case of emergency, subsequently wish to run an application on his or her land mobile radio (LMR). At present, whenever the user changes mobile devices, he or she must re-enter the identity information, for example, the user name and password, in response to prompts made by each new mobile device.

[0005] Accordingly, there is a need to enable SSO across a plurality of mobile devices to reduce the amount of time and the annoyance of having to log in and enter the identity information each and every time that the user changes devices.

BRIEF DESCRIPTION OF THE FIGURES

[0006] The accompanying figures, where like reference numerals refer to identical or functionally similar elements throughout the separate views, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate embodiments of concepts that include the claimed invention, and explain various principles and advantages of those embodiments.

[0007] FIG. **1** is a schematic view of a system for single sign-on (SSO) collaboration among a plurality of mobile devices in accordance with the present disclosure

[0008] FIG. **2** is a message sequence chart depicting steps performed in a method of single sign-on (SSO) collaboration among a plurality of mobile devices in accordance with one embodiment of the present disclosure.

[0009] FIG. **3** is a message sequence chart depicting steps performed in a method of single sign-on (SSO) collaboration among a plurality of mobile devices in accordance with another embodiment of the present disclosure.

[0010] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been drawn to scale. For example, the dimensions and locations of some of the elements in the figures may be exaggerated relative to other elements to help to improve understanding of embodiments of the present invention.

[0011] The system and method components have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the embodiments of the present invention so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

DETAILED DESCRIPTION

[0012] One aspect of this disclosure relates to a system for single sign-on collaboration among a plurality of mobile devices. The term "collaboration" or "SSO collaboration" refers to a type of working cooperation among mobile devices, whereby a user can sign-on, or login, to a first service from a first mobile device, and leverage a set of enhanced identity management procedures to securely access the first service, as well as other services, from the first mobile device, as well as from other mobile devices, without needing to perform additional manual sign-on procedures.

[0013] The system includes a server operative for issuing a first identity token (as defined below) to subsequently authenticate a user of a first of the mobile devices to a service provider, and for generating and sending a collaboration credential to the first mobile device based on the first identity token and/or user authentication. The first mobile device is operative for sending the collaboration credential generated by the server to a second mobile device paired with the first mobile device. The server is further operative for issuing a second identity token (as defined below) to subsequently authenticate the user of the second mobile device to the service provider based on the collaboration credential received from the first mobile device, to support single sign-on collaboration for the user across the plurality of mobile devices.

The collaboration credential can be generated first, and then used by either mobile device to request a respective identity token.

[0014] Advantageously, the server configures the collaboration credential as a data structure that comprises at least one of an identification of the user, an identification of the first mobile device, an identification of which of the plurality of mobile devices are permitted to collaborate with the first mobile device, and an identification of the conditions under which the collaboration is permitted to be conducted. In one embodiment, the collaboration credential is concatenated with a message authentication data structure, such as a keyed hash, also known as a message authentication code (MAC), or a digital signature. In another embodiment, the collaboration credential is encrypted with a key known only to the server.

[0015] The server also configures each identity token as a data structure that comprises at least one of an identification of the user and an identification of the mobile device to which the respective identity token is sent. As used herein, the term "data structure" includes a list, string, array, or any complex data structure that includes files or data sets. When the data structure of the collaboration credential is a file, then the file format may be JavaScript Object Notation (JSON), XML, HTML, ASCII, Binary, or any other file format, and the file may be compressed or encrypted, in part or in whole. Computing and concatenating a MAC to a data structure is herein referred to as "MACing".

[0016] The server can constitute a single identity management server for issuing each identity token and for generating and verifying the collaboration credential. In a variant construction, the server can constitute an identity management server for issuing each identity token, and a collaboration manager server for generating and verifying the collaboration credential.

[0017] A method, in accordance with another aspect of this disclosure, of single sign-on collaboration among a plurality of mobile devices, is performed by issuing and sending a first identity token to a first of the mobile devices to subsequently authenticate a user of the first mobile device to a service provider, generating and sending a collaboration credential to the first mobile device based on the first identity token and/or user authentication, pairing the first mobile device with a second mobile device, sending the collaboration credential to the second mobile device, requesting a second identity token based on the collaboration credential, and issuing and sending a second identity token to the second mobile device to subsequently authenticate the user of the second mobile device to the service provider, for supporting single sign-on collaboration for the user across the plurality of mobile devices.

[0018] Turning now to the drawings, reference numeral **10** in FIG. **1** generally identifies a system for single sign-on collaboration for a user **50** among a plurality of his or her mobile devices, such as, by way of non-limiting example, a personal digital assistant **12**, a smartphone **14**, a desktop computer **16**, a tablet **18**, a land mobile radio (LMR) **20**, and a laptop computer **22**. Other mobile devices, and other device types, that are different from those illustrated are also contemplated by the present disclosure. Each of these mobile devices has one or more network interfaces, which may include one or more radio frequency (RF) transceivers operatively connected to a network **24**, for example, the Internet, preferably over a bi-directional wireless link, such as Wi-Fi, which is an open wireless standard for transmission of digital voice and data. The network **24** need not be a single network as illustrated, but could comprise a plurality of networks interconnected by forwarding equipment. The mobile devices **12**, **14**, **16**, **18**, **20** and **22** not only communicate over the network **24** with a service provider (SP) **52**, but can also wirelessly communicate with one another, for example, via Bluetooth®, which is another open wireless standard for transmission of digital voice and data between devices.

[0019] In one embodiment, all of the user's mobile devices **12**, **14**, **16**, **18**, **20** and **22** can communicate directly with each other. In another embodiment, some of the user's mobile devices may have to communicate with each other via one or more of the user's other mobile devices. In one embodiment, all of the user's mobile devices have the same wireless interface, such as Bluetooth®. In another embodiment, some of the user's mobile devices have one wireless interface, such as Bluetooth®; others of the mobile devices have another wireless interface, such as Wi-Fi; and still others of the mobile devices have both, or other interfaces.

[0020] The system **10** includes a server **30**, which comprises either a single identity management server (IdM) **26**, as described below in connection with FIG. **2**, or the IdM **26** in combination with a collaboration manager server (CM) **28**, as described below in connection with FIG. **3**. The server **30** is operatively connected to the network **24** over a bi-directional link, which may be wired or wireless, and interacts with one or more of the devices **12**, **14**, **16**, **18**, **20** and **22**, as described in detail below. Each server comprises one or more processes running on one or more computers.

[0021] Each of the server **30** and the mobile devices **12**, **14**, **16**, **18**, **20** and **22** includes a processor, such as one or more microprocessors, microcontrollers, digital signal processors (DSPs), combinations thereof or such other devices known to those having ordinary skill in the art. The particular operations/functions of the processor, and respectively thus of the server and mobile devices, is determined by an execution of software instructions and routines that are stored in a respective at least one memory device associated with the processor, such as random access memory (RAM), dynamic random access memory (DRAM), and/or read only memory (ROM) or equivalents thereof, that store data and programs that may be executed by the corresponding processor. Further, in the event that the server **30** is implement as both the IdM **26** and the CM **28**, each of the IdM and the CM includes a processor whose particular operations/functions, and respectively thus of the server, is determined by an execution of software instructions and routines that are stored in a respective at least one memory device associated with the processor. Unless otherwise specified herein, the functionality described herein as being performed by the server(s) and mobile devices is implemented with or in software programs and instructions stored in the respective at least one memory device of the server(s) and mobile devices and executed by the associated processor of the server(s) and mobile devices.

[0022] Turning now to the message sequence chart of FIG. **2**, across the top of the chart, any one of the aforementioned mobile devices **12**, **14**, **16**, **18**, **20** and **22** is depicted, and hereinafter referred to, as device **1**, and any other of the aforementioned mobile devices **12**, **14**, **16**, **18**, **20** and **22** is depicted, and hereinafter referred to, as device **2**. It will be appreciated that the devices **1** and **2** may be of different types, or may be of the same type, e.g., both devices **1** and **2** may be smartphones. Also shown, across the top of the chart, is the IdM **26** and the SP **52**, e.g., a host for hosting services and applications that are provided over the network **24**. The timed

sequence in which various actions are performed is shown as one proceeds down away from the top of the chart.

[0023] Initially, the user **50** of device **1** (box **100**) is not logged into the SP **52**, and the user **50** of device **2** (box **102**) is not logged into the SP **52**. Thereupon, the user **50** of the device **1** first establishes a secure connection or "tunnel" between the device **1** and the IdM **26** (see message **104**), and then authenticates himself or herself to the IdM **26**. The user **50** inputs into the device **1**, and the device conveys to IdM **26**, identity information, for example, a user name and a user password, and, optionally, some other data, such as what other devices or types of devices to which the user **50** wants to gain access, or the conditions under which such access is to be permitted or denied.

[0024] In one embodiment, rather than explicitly entering the other devices or device types, or the conditions under which access is to be permitted, the user **50** could instead input to the device **1**, and the device conveys to IdM **26**, an indication of what actions the user **50** intends to perform, or what services/applications the user **50** intends to use. In another embodiment, data, such as the devices, the types of devices, the actions or the services/applications, is not entered by the user **50**, but instead, is automatically generated by the device **1** and is sent to the server **30**. In response to receiving the identity information from device **1**, the IdM **26** issues a first data structure (see box **106**) or first identity token **1** (as defined below) and sends the first identity token **1** to the device **1** to subsequently authenticate the user **50** of the device **1** to the SP **52** (see message **108**).

[0025] In one embodiment, the device **1** next requests from the IdM **26** a collaboration credential based on the first identity token **1** and/or user authentication (see message **110**) and that is sharable among two or more of mobile devices **12**, **14**, **16**, **18**, **20** and **22**, and more particularly between device **1** and device **2**. For example, in response to receiving the first identity token **1**, device **1** may convey, to the IdM **26**, a collaboration request that is associated with the first identity token **1**, for example, that includes the first identity token **1** or a value associated with the first identity token **1**, such as a value derived from the first identity token **1**, or where the collaboration request is secured by the first identity token, or transmitted over a link secured with the first identity token, or transited by a device which uses the first identity token to establish a secure communications session. This request can be performed automatically or manually. In response to receiving the request, the IdM **26** generates the collaboration credential (see box **112**) as a data structure, and sends the collaboration credential to the device **1** (see message **114**). In another embodiment, rather than sending the first identity token **1** and the collaboration credential as independent actions, the IdM **26** may send the collaboration credential to device **1** simultaneously with the first identity token **1**, for example, in a same message, in response to authenticating the user of device **1**.

[0026] In one embodiment, the collaboration credential is a Kerberos data structure or ticket containing, by way of non-limiting example, one or more of a user identification, a session identification, a collaboration device identification (s), other collaboration device description(s), an expiration time, and other usage constraints. In another embodiment, the collaboration credential is an OAuth token, a SAML token, a JSON Web Token (JWT), or another type of identity token. In one embodiment, the collaboration credential is a data structure that contains information used to bind multiple devices to a single user **50**, or to bind multiple devices to a single purpose, or to bind the user **50** to a device, or to bind a device to one or more other devices, or to bind at least one device to a user group. The device **1** now knows which of the plurality of mobile devices **12**, **14**, **16**, **18**, **20** and **22** are permitted to collaborate with the device **1**, and also knows the conditions under which such collaboration is permitted to be conducted.

[0027] By way of non-limiting example, the device **1** might be instructed by the collaboration credential to collaborate with only one other device, such as the user's desktop computer **16**, or to only collaborate with another device for a set period of time, or to only collaborate using certain applications hosted by the SP **52**, or to collaborate only with mobile devices with which it is able to perform certificate-based authentication, etc. The data contained in the collaboration credential may have been supplied by the user **50**, or by the device **1**, during identification/authentication as described above, or may have been entered into a database of the server **30** beforehand. In one embodiment, the data provided by the user **50** may be used in conjunction with data in the aforementioned database to determine the conditions under which collaboration is permitted.

[0028] Next, a transport layer security (TLS) session is established between the device **1** and the SP **52** (see message **116**). Cryptographic protocols, other than TLS, such as Internet Protocol Security (IPsec), Secure Sockets Layer (SSL), Secure Shell (SSH), and like cryptographic protocols that provide communication security over the Internet, could also be employed. Alternatively, no cryptographic protocol between the device **1** and the SP **52** could be used. The device **1** requests service based on the first identity token **1** (see message **118**). In response, the SP **52** activates the service and/or associated application and allows device **1** access to the service/application (see message **120**). The user **50** is now authenticated and logged into the SP **52** (see box **122**).

[0029] When collaboration with another device, that is, the device **2**, is desired, the devices **1** and **2** must establish a security association between each other. When such collaborating devices form such a security association, they are said to be paired. If Bluetooth® is employed, then pairing occurs when two Bluetooth® devices agree to communicate with each other and establish a secure connection. In some cases, Bluetooth® can provide the needed security association, and in other cases a higher communication layer can provide the needed security association. In some cases, a shared secret, also sometimes referred to as a passkey or a personal identification number (PIN), is exchanged between the two devices **1** and **2**. Alternatively, the devices **1** and **2** can each derive a shared secret without directly exchanging the value of the shared secret between each other, such as is provided by the well known Diffie-Hellman algorithm.

[0030] A passkey is a code shared by both devices **1** and **2**, which proves that both devices have agreed to pair with each other. Once paired (see message **124**), the device **1** is operative for sending the collaboration credential (see box **126**) generated by the server **30** to the device **2** (see message **128**). The pairing need not be performed immediately prior to the sharing of the collaboration credential, but could be performed beforehand. It will be appreciated by those skilled in the art that once a security association exists between devices, data can be sent securely between the devices using the security association.

[0031] In one embodiment the security association used for collaborative pairing is established through the use of certifi-

cate-based authentication. Where the collaborating devices exchange digital certificates, such as standard X.509 certificates, public key cryptographic methods, such as those described by the TLS standard, are used to establish the necessary security association. In one embodiment, attributes in the exchanged certificates can be used determine the applicability of SSO collaboration for the device presenting the certificate.

[0032] In one embodiment, the device **1** sends a collaboration notification (see message **125**) to the server **30** to indicate that it has sent, or will send, the collaboration credential to the device **2**. The collaboration notification is a message, file or data structure, which identifies the device **1** as the source of the collaboration credential, and identifies the device **2** as the recipient of the collaboration credential. The collaboration notification may further contain scoping assertions about the intended use of the collaboration credential. For example, the scoping assertions may indicate that the collaboration credential may only be used for services specifically identified in the collaboration notification. In one embodiment, the collaboration notification may be sent to the device **2** by the device **1**, after which the device **2** forwards the collaboration notification to the server **30**.

[0033] Next, a TLS session is established between the device **2** and the IdM **26** (see message **130**). The device **2** next requests a second data structure or second identity token **2** (as defined below) based on the collaboration credential (see message **132**). In response, the IdM **26** verifies the collaboration credential (see box **134**), and issues and sends to device **2** the second identity token **2** (see message **136**), which second identity token subsequently is used to authenticate the user of the device **2** to the SP **52**. In one embodiment, when the IdM **26** verifies the collaboration credential, the IdM **26** will compare the identity of the device from which it received the collaboration credential (i.e., the device **2**) with any collaboration notification received from the device **1**. In one embodiment, the second identity token **2** identifies the same user **50** as the first identity token **1**. The collaboration credential can be generated first, and then used by either mobile device **1** or **2** to request a respective identity token **1** or **2**.

[0034] Next, a TLS session is established between the device **2** and the SP **52** (see message **138**). The device **2** requests service based on the second identity token **2** and/or user authentication (see message **140**). In response, the SP **52** activates the service/application and allows device **2** access to the service/application (see message **142**), thereby enabling single sign-on collaboration for the user **50** across the devices **1** and **2**. The user **50** is now authenticated and logged into the SP **52** (see box **144**). If additional collaboration is required for an additional one of the aforementioned devices **12**, **14**, **16**, **18**, **20** and **22**, then the above-described process is repeated. It will be noted that the identity tokens **1** and **2** are not shared; only the collaboration credential is passed between the devices **1** and **2**.

[0035] FIG. **3** is analogous to FIG. **2**, except that the SP **52** has been omitted for ease of illustration, and, instead of the server **30** just constituting the IdM **26**, the server **30** now comprises the IdM **26** and the CM **28**. This embodiment allows the potential re-use of a commercial-off-the-shelf (COTS) IdM **26**. In brief, the IdM **26** still issues identity tokens, as described above, but now the CM **28** generates and verifies the collaboration credential.

[0036] As shown in FIG. **3**, the user **50** of device **1** (box **200**) is not logged into the SP **52**, and the user **50** of device **2** (box **202**) is not logged into the SP **52**. The user **50** then logs into the device **1** (box **204**), and establishes a secure connection or "tunnel" between the device **1** and the IdM **26** as described with respect to FIG. **2**. The user **50** then enters the user's identification data into device **1** and the device conveys the identification data as described with respect to FIG. **2** to the IdM **26** (see message **206**). In response to receiving the identification data, the IdM **26** issues the first identity token **1** (see box **208**) and sends the first identity token **1** to the device **1** (see message **210**) for use in subsequently authenticatating the user **50** of the device **1** to the SP **52**.

[0037] The device **1** next requests, from the CM **28**, the collaboration credential based on the first identity token **1** and/or user authentication (see message **212**). The CM **28** verifies the first identity token **1** (see message **214**) after which the CM **28** generates the collaboration credential (see box **214**) and sends the collaboration credential to the device **1** (see message **218**). Verifying the first identity token **1** by the CM **28** may involve performing MAC or signature verification, or may require an explicit request to the IdM **26**. The user **50** is now able to log into, and be authenticated to, the SP **52** via the device **1** (see box **220**).

[0038] The devices **1** and **2** are paired (see message **222**), as described with respect to FIG. **2**, after which the device **1** (see box **224**) is operative for sending the collaboration credential to the device **2** (see message **226**). Next, a secure tunnel is established between the device **2** and the CM **28** (see message **228**). The device **2** next requests, from the CM **28**, the second identity token **2** based on the collaboration credential (see message **230**). In response, the CM **28** verifies the collaboration credential (see box **232**), and sends the request for the second identity token **2** to the IdM **26** (see message **234**). In response to receiving the request from the CM, the IdM **26** issues the second identity token **2** (see box **236**) and sends the second identity token **2** to the CM **28** (see message **238**), which, in turn, sends the second identity token **2** to the device **2** (see message **240**) for use in subsequently authenticating the user **50** of the device **2** to the SP **52**. The same user **50** is now able to be logged into, and be authenticated to, the SP **52** via the device **2** (see box **242**).

[0039] In a preferred embodiment, rather than having the device **2** request the second identity token **2** from the CM **28**, the device **2** can directly request the identity token **2** from the IdM **26**. Also, rather than having the IdM **26** send the second identity token **2** to the CM **28**, the IdM **26** can directly send the second identity token **2** to the device **2**. Further, in the preferred embodiment, the identity token is an OAuth token, and the collaboration credential is an OAuth Request with a grant type equal to a SAML assertion or a JWT assertion.

[0040] As described so far, the collaboration credential is the same for all the devices. It is also contemplated that different collaboration credentials could be used for different sets of the devices. For example, one collaboration credential can be used by the device **1** to enable SSO collaboration with other devices, and a separate collaboration credential can be used by device **2** to collaborate with other devices. Alternatively, one collaboration credential may be constrained to a specific application, a set of applications, a device type, a device assurance level, a collaborative network type (personal area network, vehicular area network, etc.), or to any other device, user, or network attribute. The collaboration credential can be generated first, and then used by either mobile device to request a respective identity token.

[0041] Throughout this specification, the term "identity token" is used to refer to a syntactical structure that communicates information about the user **50**. Types of information often communicated within an identity token include: a unique identifier for the user **50**, a unique identifier of the server **30** which issued the identity token, an expiration time after which the identity token may no longer be used, the time at which the identity token was issued, and a primary authentication context reference specifying the time at which the user authenticated themselves in order to obtain the identity token and the method of authentication they used (passwords and RSA passcodes are two examples).

[0042] Identity tokens may also contain other relevant attributes about the user **50**, such as his or her agency of employment, roles within his or her agency, special skills, or identifying facial attributes. This list is meant to be exemplary of a typical identity token, and non-binding, as many other attributes might be included as well. Identity tokens may be either digitally signed by the token issuer, or may alternatively require a secure connection between the consumer of the identity token (often referred to as the relying party, service provider, or resource server) and the identity token issuer.

[0043] Identity tokens are also known by other names within industry and standards. In the SAML 2.0 protocol, identity tokens may be referred to as SAML assertions, or simply, identity assertions. In OAuth, identity tokens are referred to as access tokens, and in OpenID Connect, identity tokens may be referred to as id tokens. Other identity tokens are intended for usage strictly between the user and the token issuing server, and these are often referred to as session tokens. In OAuth, a refresh token could be thought of as but one example of a session token.

[0044] In the foregoing specification, specific embodiments have been described. However, one of ordinary skill in the art appreciates that various modifications and changes can be made without departing from the scope of the invention as set forth in the claims below. For example, although the TLS protocol has been described and illustrated herein, other cryptographic protocols, such as Internet Protocol Security (IPsec), Secure Sockets Layer (SSL), Secure Shell (SSH), and like cryptographic protocols that provide communication security over the Internet, could be employed. Accordingly, the specification and figures are to be regarded in an illustrative rather than a restrictive sense, and all such modifications are intended to be included within the scope of present teachings.

[0045] The benefits, advantages, solutions to problems, and any element(s) that may cause any benefit, advantage, or solution to occur or become more pronounced are not to be construed as a critical, required, or essential features or elements of any or all the claims. The invention is defined solely by the appended claims including any amendments made during the pendency of this application and all equivalents of those claims as issued.

[0046] Moreover in this document, relational terms such as first and second, top and bottom, and the like may be used solely to distinguish one entity or action from another entity or action without necessarily requiring or implying any actual such relationship or order between such entities or actions. The terms "comprises," "comprising," "has," "having," "includes," "including," "contains," "containing," or any other variation thereof, are intended to cover a non-exclusive inclusion, such that a process, method, article, or system that comprises, has, includes, contains a list of elements does not include only those elements, but may include other elements not expressly listed or inherent to such process, method, article, or system. An element proceeded by "comprises . . . a," "has . . . a," "includes . . . a," or "contains . . . a," does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or system that comprises, has, includes, or contains the element. The terms "a" and "an" are defined as one or more unless explicitly stated otherwise herein. The terms "substantially," "essentially," "approximately," "about," or any other version thereof, are defined as being close to as understood by one of ordinary skill in the art, and in one non-limiting embodiment the term is defined to be within 10%, in another embodiment within 5%, in another embodiment within 1%, and in another embodiment within 0.5%. The term "coupled" as used herein is defined as connected, although not necessarily directly and not necessarily mechanically. A device or structure that is "configured" in a certain way is configured in at least that way, but may also be configured in ways that are not listed.

[0047] It will be appreciated that some embodiments may be comprised of one or more generic or specialized processors (or "processing devices") such as microprocessors, digital signal processors, customized processors, and field programmable gate arrays (FPGAs), and unique stored program instructions (including both software and firmware) that control the one or more processors to implement, in conjunction with certain non-processor circuits, some, most, or all of the functions of the method and/or system described herein. Alternatively, some or all functions could be implemented by a state machine that has no stored program instructions, or in one or more application specific integrated circuits (ASICs), in which each function or some combinations of certain of the functions are implemented as custom logic. Of course, a combination of the two approaches could be used.

[0048] Moreover, an embodiment can be implemented as a computer-readable storage medium having computer readable code stored thereon for programming a computer (e.g., comprising a processor) to perform a method as described and claimed herein. Examples of such computer-readable storage mediums include, but are not limited to, a hard disk, a CD-ROM, an optical storage device, a magnetic storage device, a ROM (Read Only Memory), a PROM (Programmable Read Only Memory), an EPROM (Erasable Programmable Read Only Memory), an EEPROM (Electrically Erasable Programmable Read Only Memory) and a Flash memory. Further, it is expected that one of ordinary skill, notwithstanding possibly significant effort and many design choices motivated by, for example, available time, current technology, and economic considerations, when guided by the concepts and principles disclosed herein, will be readily capable of generating such software instructions and programs and ICs with minimal experimentation.

[0049] The Abstract of the Disclosure is provided to allow the reader to quickly ascertain the nature of the technical disclosure. It is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims. In addition, in the foregoing Detailed Description, it can be seen that various features are grouped together in various embodiments for the purpose of streamlining the disclosure. This method of disclosure is not to be interpreted as reflecting an intention that the claimed embodiments require more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive subject mat-

ter lies in less than all features of a single disclosed embodiment. Thus, the following claims are hereby incorporated into the Detailed Description, with each claim standing on its own as a separately claimed subject matter.

1. An apparatus for enabling a user of a first mobile device to extend user authentication credentials to a second mobile device, the apparatus comprising:

a server having a processor that is configured to:

issue and send a first identity token to the first mobile device, wherein the first identity token can be utilized to authenticate the user of the first mobile device to a service provider;

generate a collaboration credential, wherein generation of the collaboration credential is based on one or more of user authentication and receipt of a collaboration request associated with the first identity token and wherein the collaboration credential is sharable among a plurality of mobile devices;

send the collaboration credential to the first mobile device;

receive the collaboration credential from the second mobile device;

verify the collaboration credential received from the second mobile device; and

in response to verifying the collaboration credential received from the second mobile device, issue and send a second identity token to the second mobile device, wherein the second identity token can be utilized to authenticate the second mobile device to the service provider.

2. The apparatus of claim **1**, wherein the processor is configured to receive the collaboration request from the first mobile device and wherein the processor is configured to generate the collaboration credential in response to receiving the collaboration request.

3. The apparatus of claim **1**, further comprising the first mobile device, wherein the first mobile device is configured to:

receive the first identity token and the collaboration credential from the server; and

send the collaboration credential to the second mobile device.

4. The apparatus of claim **3**, further comprising the second mobile device, wherein the second mobile device is configured to:

receive the collaboration credential from the first mobile device;

send the collaboration credential to the server; and

in response to sending the collaboration credential, receive the second identity token.

5. The apparatus of claim **1**, wherein the processor further is configured to receive the collaboration credential from a third mobile device and, in response to receiving the collaboration credential from the third mobile device, issue and send a third identity token to the third mobile device, wherein the third identity token can be utilized to authenticate the user of the third mobile device to the service provider.

6. The apparatus of claim **1**, wherein the processor further is configured to receive, from the first mobile device and in response to sending the collaboration credential to the first mobile device, a collaboration notification that identifies the first mobile device as a source of the collaboration credential and identifies the second mobile device as a recipient of the collaboration credential.

7. The apparatus of claim **1**, wherein the processor further is configured to configure the collaboration credential as a data structure comprising at least one of an identification of the user, an identification of the first mobile device, an identification of which of a plurality of mobile devices are permitted to collaborate with the first mobile device, and an identification of the conditions under which the collaboration is permitted to be conducted.

8. The apparatus of claim **1**, wherein the processor further is configured to configure each identity token as a data structure comprising at least one of an identification of the user and an identification of the mobile device to which the respective identity token is sent.

9. The apparatus of claim **1**, wherein the server comprises an identity management server that is configured to issue each identity token and generate and verify the collaboration credential.

10. The apparatus of claim **1**, wherein the server comprises:

an identity management server that is configured to issue each identity token; and

a collaboration manager server that is configured to generate and verify the collaboration credential.

11. A method for enabling a user of a first mobile device to extend user authentication credentials to a second mobile device, the method comprising:

issuing and sending a first identity token to the first mobile device, wherein the first identity token can be utilized to authenticate the user of the first mobile device to a service provider;

generating a collaboration credential, wherein generation of the collaboration credential is based on one or more of user authentication and receipt of a collaboration request associated with the first identity token and wherein the collaboration credential is sharable among a plurality of mobile devices;

sending the collaboration credential to the first mobile device;

receiving the collaboration credential from the second mobile device;

verifying the collaboration credential received from the second mobile device; and

in response to verifying the collaboration credential received from the second mobile device, issuing and sending a second identity token to the second mobile device, wherein the second identity token can be utilized to authenticate the second mobile device to the service provider.

12. The method of claim **11**, wherein the method further comprises receiving the collaboration request from the first mobile device and wherein generating the collaboration credential comprises generating the collaboration credential in response to receiving the collaboration request.

13. The method of claim **11**, further comprising:

receiving, by the first mobile device, the first identity token and the collaboration credential from the server; and

sending, by the first mobile device, the collaboration credential to the second mobile device.

14. The method of claim **13**, further comprising:

receiving, by the second mobile device, the collaboration credential from the first mobile device;

sending, by the second mobile device to the server, the collaboration credential; and

in response to sending the collaboration credential, receiving, by the second mobile device, the second identity token.

15. The method of claim **11**, further comprising:

receiving the collaboration credential from the third mobile device; and

in response to receiving the collaboration credential from the third mobile device, issuing and sending a third identity token to the third mobile device, wherein the third identity token can be utilized to authenticate the user of the third mobile device to the service provider.

16. The method of claim **11**, further comprising, in response to sending the collaboration credential to the first mobile device, receiving a collaboration notification that identifies the first mobile device as a source of the collaboration credential and identifies the second mobile device as a recipient of the collaboration credential.

17. The method of claim **11**, further comprising configuring the collaboration credential as a data structure comprising at least one of an identification of the user, an identification of the first mobile device, an identification of which of a plurality of mobile devices are permitted to collaborate with the first mobile device, and an identification of the conditions under which the collaboration is permitted to be conducted.

18. The method of claim **11**, further comprising configuring each identity token as a data structure comprising at least one of an identification of the user and an identification of the mobile device to which the respective identity token is sent.

19. An apparatus for enabling single sign-on collaboration among a plurality of mobile devices, the apparatus comprising:

a mobile device comprising a processor that is configured to:

receive each of a first identity token and a collaboration credential from a server, wherein the first identity token can be utilized to authenticate a user of the mobile device to a service provider and wherein the collaboration credential is sharable among a plurality of mobile devices and may be utilized to provide an identity token to each mobile device of the plurality of mobile devices; and

send the collaboration credential to another mobile device.

20. The apparatus of claim **19**, wherein the processor is configured to receive the collaboration credential by sending a collaboration request to the server, wherein the collaboration request is associated with the first identity token, and, in response to sending the collaboration request, receive the collaboration credential.

21. The apparatus of claim **19**, wherein the mobile device is a first mobile device and wherein the apparatus further comprises a second mobile device that is configured to:

receive the collaboration credential from the first mobile device;

send the collaboration credential to the server; and

in response to sending the collaboration credential, receive the second identity token from the server, wherein the second identity token can be utilized to authenticate the user of the second mobile device to the service provider.

22. The apparatus of claim **19**, wherein the processor further is configured to, in response to receiving the collaboration credential, send a collaboration notification to the server, wherein the collaboration notification identifies the mobile device as a source of the collaboration credential and identifies the another mobile device as a recipient of the collaboration credential.

23. A method for enabling single sign-on collaboration among a plurality of mobile devices, the method comprising:

receiving, by a mobile device of the plurality of communication devices, each of a first identity token and a collaboration credential from a server, wherein the first identity token can be utilized to authenticate a user of the mobile device to a service provider and wherein the collaboration credential is sharable among a plurality of mobile devices and may be utilized to provide an identity token to each mobile device of the plurality of mobile devices; and

sending, by the mobile device, the collaboration credential to another mobile device of the plurality of mobile devices.

24. The method of claim **23**, wherein receiving the collaboration credential comprises:

sending a collaboration request to the server, wherein the collaboration request is associated with the first identity token; and

in response to sending the collaboration request, receiving the collaboration credential.

25. The method of claim **23**, wherein the method further comprises, in response to receiving, by the mobile device, the collaboration credential, sending a collaboration notification to the server, wherein the collaboration notification identifies the mobile device as a source of the collaboration credential and identifies the another mobile device as a recipient of the collaboration credential.

* * * * *