Innovation, Sciences et Développement économique Canada
Office de la Propriété Intellectuelle du Canada

Innovation, Science and Economic Development Canada
Canadian Intellectual Property Office

CA 2995394 C 2024/01/16

(11)(21) **2 995 394**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2016/08/12
(87) **Date publication PCT/PCT Publication Date:** 2017/02/16
(45) **Date de délivrance/Issue Date:** 2024/01/16
(85) **Entrée phase nationale/National Entry:** 2018/02/12
(86) **N° demande PCT/PCT Application No.:** AU 2016/000275
(87) **N° publication PCT/PCT Publication No.:** 2017/024335
(30) **Priorité/Priority:** 2015/08/12 (AU2015903231)

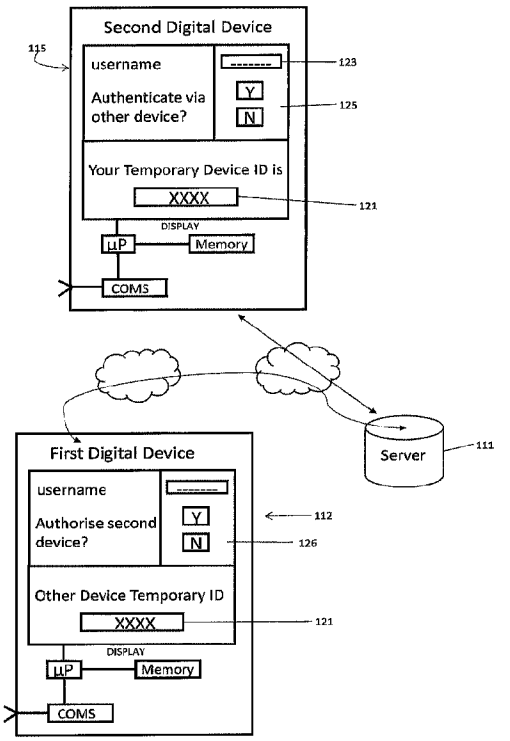
(51) **Cl.Int./Int.Cl.** ***G06F 21/31*** (2013.01)

(72) **Inventeur/Inventor:**
RICHARDSON, RIC B., AU

(73) **Propriétaire/Owner:**
HAVENTEC PTY LTD, AU

(74) **Agent:** BORDEN LADNER GERVAIS LLP

(54) **Titre : SYSTEME D'AUTHENTIFICATION DE DISPOSITIFS**
(54) **Title: SYSTEM OF DEVICE AUTHENTICATION**



(57) **Abrégé/Abstract:**
There is disclosed a method of authenticating a user with respect to more than one digital device; said user having an account on a server; said method comprising: using a temporary unique ID to permit the user to determine whether to agree to an authentication request and communicating agreement or otherwise by communication effected from a first digital device to the server. Also disclosed is an apparatus for effecting authentication of at least a second device with respect to a server environment where authentication of a first device has been effected.

ABSTRACT

There is disclosed a method of authenticating a user with respect to more than one digital device; said user having an account on a server; said method comprising: using a temporary unique ID to permit the user to determine whether to agree to an authentication request and communicating agreement or otherwise by communication effected from a first digital device to the server. Also disclosed is an apparatus for effecting authentication of at least a second device with respect to a server environment where authentication of a first device has been effected.

Date Reçue/Date Received 2023-02-14

System of Device Authentication

Background

[0001] Many efforts have been made to try and simplify the process of authentication of a person's identity over the years. One system, known as oAuth allows a person to authenticate with a site but then share those authentication credentials with other sites and services using tokens that expire over time.

[0002] One key advantage of this approach is that a person may only be required to authenticate their identity with one site but have access to multiple sites without the inconvenience of setting up and undergoing a separate authentication process for each site.

[0003] A disadvantage of this system is that it is not typically possible to use the same approach to authenticate users that connect from different devices while using the same account.

[0004] Whilst there are known mechanisms for a user to share data amongst multiple digital devices such as for example disclosed in US 2011/0138018 to QUALCOMM Incorporated, there is currently no mechanism for that user to cause consequential authentication based on an initial authentication on a first device.

[0005] This capability would be highly desirable in that an authentication on one of the user's devices for a site account could be used across multiple devices that the user owns or uses.

[0006] Embodiments of the present invention seek to address this problem or at least provide a useful alternative.

Date Reçue/Date Received 2023-02-14

Notes

[0007] The term "comprising" (and grammatical variations thereof) is used in this specification in the inclusive sense of "having" or "including", and not in the exclusive sense of "consisting only of".

[0008] The above discussion of the prior art in the Background of the invention, is not an admission that any information discussed therein is citable prior art or part of the common general knowledge of persons skilled in the art in any country.

Brief Description of Invention

Definitions:

[0009] Authentication: In this specification, authentication is used in the sense of taking steps to further identify a user log-in usually but not exclusively in a client server environment. Examples of the steps include requiring submitting a passcode which has previously been identified as associated with the user log-in. In other non-exclusive forms, biometric data may be required to effect the step to further identify a user log-in. Authentication is established at the software level as it necessarily involves a level of selectivity as to what data or categories of data are available for communication subsequent to authentication.

[00010] Trust: In this specification, trust refers to a relationship that can be established between two digital devices for the purpose of transmitting data between them. The trust may be at a hardware level.

Date Reçue/Date Received 2023-02-14

[00011] Accordingly, in one broad form of the invention, there is provided a method of authenticating a user with respect to more than one digital device; said user having an account on a server; said method comprising

a. the user effecting a login sequence and an authenticating sequence on a first digital device as referenced and recorded on the server thereby to authenticate the user with respect to the first digital device;
b. the user subsequently effecting a login sequence on a second digital device; the second digital device communicating the user login sequence to the server;
c. the server communicating an option to the second digital device to utilise the first digital device to effect authentication of the user with respect to the second digital device;
d. on receipt of a request from the second digital device to effect authentication by use of the first digital device:
    i. the server issuing a temporary unique ID to the second digital device;
    ii. the server sending an authentication request to the first digital device;
    iii. the authentication request including transmission of the temporary unique ID issued to the second digital device;
    iv. communicating the temporary unique ID from the first digital device to the user thereby to permit the user to determine whether to agree to the authentication request;
    v. the user communicating agreement or otherwise by communication effected from the first digital device to the server.

[00012] In yet a further broad form of the invention, there is provided a method of authenticating a user session instigated by a user on a digital device with respect to a given user login identity on a server; said method comprising:

Date Reçue/Date Received 2023-02-14

a. authenticating a first digital device for a first user login identity as recorded on the server;
b. thereby to commit transfer of protected data between the first digital device and the server;
c. subsequently authenticating a second digital device for said first user login identity as recorded on said server by the steps of:
d. said user entering said first user login identity on said second digital device;
e. said second digital device being issued by said server with a temporary identifier in response to said user entering said first user login identity on said second digital device;
f. said server then transmitting said temporary identifier to said first digital device for communication to said user by said first digital device;
g. said user responding to said communication of said temporary identifier to said user by said first digital device by causing said first digital device to communicate an authorise said second digital device command to said server if a response condition is satisfied;

whereby said first user login identity is authorised for said second digital device.

[00013] In yet a further broad form of the invention, there is provided in an environment where a first device may communicate with a server subject to authentication of the device with respect to the server, a method of authenticating a second device with respect to the server; said method comprising:

a. On request, the server communicating an identifier to the second device and the first device;
b. Authenticating the second device to the same level as the first device subject to a confirmation step.

[00014] In yet a further broad form of the invention, there is provided an apparatus for effecting authentication of at least a second device with respect to a server environment where authentication of a first device has been effected; the apparatus including:

a. A memory storing at least a first log-in identifier and an associated authenticating data item
b. A processor which generates a temporary identifier as a first step in effecting authentication of at least the second device
a. A transmitter which transmits the temporary identifier to the at least a second device and to the first device.
b. A comparison device which compares the temporary identifier of the first device and of the second device and makes a decision based on the comparison as to whether to permit the server to authenticate the second device with respect to the server environment.

[00015] Preferably said response condition is a positive comparison of the temporary identifier communicated by said first digital device with the temporary identifier communicated to said second digital device by said server.

[00016] Preferably the temporary identifier is an alphanumeric sequence.

[00017] Preferably protected data is data stored with respect to said first user login on said server.

[00018] Preferably protected data is application data stored with respect to said first user login on said server.

[00019] Preferably authentication of said first digital device is effected by entry of a user login identifier and separate authenticating data into said first digital device.

Date Reçue/Date Received 2023-02-14

[00020] Preferably said separate authenticating data is a password.

[00021] Preferably said separate authenticating data is biometric data.

[00022] Preferably, the confirmation step comprises comparing the identifier on the second device and the identifier on the first device.

[00023] Preferably, confirmation is effected if, and only if, the identifier on the second device matches with the identifier on the first device

[00024] Preferably, the identifier is an alpha-numeric sequence.

[00025] Preferably authentication may be established for a single session.

[00026] Preferably authentication may be established for a limited number of sessions

[00027] Preferably authentication may be established for an indefinite period

[00028] In yet a further broad form of the invention, there is provided media encoded with code which, when executed by a processor, performs the method as described above.

Brief Description of Drawings

[00029] Embodiments of the present invention will now be described with reference to the drawings wherein:

[00030] Figure 1A – Illustrates a prior art hardware trust establishment system.

[00031] Figure 1B – Illustrates main components of an example embodiment.

[00032] Figure 2 is a flow diagram of steps effected by the example of Figure 1B.

[00033] Figure 3 is a block diagram illustrating interaction between a first digital device and a second digital device operable according to an embodiment of the system of the present invention.

[00034] Figure 4 is a block diagram illustrating an example of the interaction of Figure 3 as experienced by a user.

Detailed Description and Operation

[00035] Figure 1A illustrates diagrammatically a prior art "Bluetooth™" arrangement for establishing a data connection between two devices sufficient to establish a basic level of trust. This system operates direct between two devices and, in essence, is a mechanism to ensure that the two devices between which communication is desired are unambiguously identified in order to provide trust at the hardware level.

[00036] Embodiments of the present invention seek to provide the ability to authenticate a second or more device with respect to a server environment relying on authentication having first been established for a first device with respect to the same server environment. In preferred forms, but not exclusively, the server environment is defined by way of user log-in.

[00037] Figure 1B discloses the main components of an example embodiment of the present invention. Initially a user 10 would set up an authenticated

connection to a server 11 enabled with the example embodiment using authentication methods known in the art.

[00038] To authenticate the user 10 and the user's first digital device 12, in this case a smartphone, the user uses a web-enabled application 17 to register with the server 11. In this instance this device 12 would be registered as the user's primary reference or vouching device.

[00039] The identity 14 of the device 12 is stored with the user's account 13 and can be referenced in the future when the user requires additional devices that they own or use to be authenticated with the server 11.

[00040] The user's account 13 also includes an account ID or name or username 16 which can be used to uniquely identify and name the user of the account.

[00041] When the user 10 wishes to authenticate themselves using a new device 15, the user connects the device 15 to the server 11 over a public network such as the Internet 20 using an application such as a web browser 16 and then enters their account name 16 to identify themselves as user 10 to the server 11.

[00042] The server 11 then notifies the user 10 that their second device is not yet recognised as an authenticated device and asks the user 10 if they would like to add the device to their account 13.

[00043] Upon agreeing to proceed, the user is presented with a button to initiate a request from the server 11 to the user's primary vouching device 12 to verify an authenticated connection between the user 10 and the server 11. The user is also presented with a device identification such as a four digit number 18 which can be used to identify the device.

[00044] Subsequently the second digital device 15 displays a screen 21 explaining to the user that they will need to obtain authentication from their vouching device in order to proceed with authenticating their new device 15. They will also be shown temporary ID 21 preferably in the form of a four-digit number that is generated new each time a new device requests authentication. This four-digit number is generated by the server 11 and is used once to identify the requesting device 15 to the vouching device 12 when an authentication request is made.

[00045] The new device 15 then goes into a waiting mode to receive an authentication verification from the server 11 after the vouching device 12 has been used to verify your identity.

[00046] At the same time the server 11 is prompted to initiate a connection with the user's primary first digital vouching device 12 to verify and authorise the user's authentication request.

[00047] In the case of a smartphone such as an Apple iPhone™, a notification message can be then sent to the user's device 12, which in turn can open the user's application 17 to verify the users identity.

[00048] If the application's 17 connection to the server 11 is current and not expired the user is then shown the four-digit number that identifies the requesting device and the user is prompted on screen to authorise the new device after verifying the identity of the new device.

[00049] If the application's 17 connection to the server 11 is not current and not expired the user is then asked to authenticate using the vouching device 12. Subsequently the user is shown the four-digit number that identifies the

requesting device and the user is prompted on screen to authorise the new device after verifying the identity of the new device.

[00050] Once the server 11 receives a verification of the identity of the new device 15, the server allows an authenticated session to proceed between the new device 15 and the server 11.

[00051] The screen of the new device 15 notifies the user that the authentication has been completed successfully and access to the site is enabled. Additionally a new device identity 19 is added to the user's account 13 on the server 11.

[00052] Figure 2 discloses an example control process of the example embodiment. The process involves an initial device being used by a user 40, a server 41 with which the user desires to connect, and a second device 42 that the user wants to authenticate with their account on the server.

[00053] Initially a user establishes an authenticated account with the server 43 and the server stores the account details for future authentication 44.

[00054] Subsequently a user may request that a new device be authenticated by the user 45 to use the same account on the server. To identify themselves to the server the user enters their username 46 and submits it for use by the server.

[00055] The server then confirms that the username is known but recognises that the device being used by the user is not known to the server 47. The server then asks the user if they want to use the authentication credentials of an existing device 48 to vouch for the new device to be recognised with the account. If the user agrees 49 then the server gives the requesting device a temporary unique identity 50 which is then shown to the user on the new

device screen 51. The new device then goes into a waiting mode 53 until the request to receive an authentication is answered.

[00056] The server 41 then sends an authentication request 52 for the new device to the vouching device 40 which is already authenticated and in use or can use existing authentication credentials to establish and authenticate it and the users identity.

[00057] The authentication request is received by the existing device along with the identity of the requesting device 54. This step is important in that it allows the user to properly identify the device that is being used to request an new authentication.

[00058] The user then confirms the identity of the requesting device and allows authentication of the new device to proceed 55. Subsequently the server receives the authorisation to authenticate the user on the new device 56 and the server shares authentication credentials with the new device 57.

[00059] As a result the new device receives the authentication credentials 58 and the new device is allowed to be used to access the users account from the new device 59.

[00060] The result is an authentication system that allows authenticated credentials from a known device to be shared with a new device to allow it to access the same account and resources.

[00061] Figures 3 and 4 are block diagrams illustrating interaction between a first digital device and a second digital device operable according to an embodiment of the system of the present invention.

[00062] With reference to Figure 3 where like components are numbered as for earlier embodiments except in the 100s series, there is shown a first digital device 112 (ID 0) in communication with a server 111 whereby a user 110 may "log-in" by way of an application running on digital device 112 to an user account 113 on server 111. In order for data or applications associated with the user account 113 to be communicated to digital device 112 the user log-in must be authenticated by the server 111. In this case, the step of authentication is provided by the user entering a username 123 and an associated password 124. If these match then authentication has occurred and a user session may operate between the first digital device 112 and the server 111.

[00063] In accordance with an embodiment of the present invention, if the user wishes to authenticate a second digital device 115 (ID 1) with respect to the same user account 113, this may be effected by entering the same username 123 into an application on second digital device 115 thereby to trigger a log-in sequence to the server 111.

[00064] As illustrated in Figure 4, in use, the user may be asked to elect whether to authenticate via another device, for example via choice check-box 125.

[00065] In the event the user does elect to authenticate via another device, server 111 generates and issues a temporary ID 121 to second digital device 115. The temporary ID 121 is then displayed on second digital device 115 or is otherwise made available for communication to the user sufficient for the user to verify the temporary ID 121 which has been issued for the second digital device 115.

[00066] At the same time, subsequently, server 111 issues the same temporary ID 121 to first digital device 112. Again, the first digital device 112 causes the temporary ID 121 to be displayed on first digital device 112 or

otherwise made available for communication to the user sufficient for the user to verify the temporary ID 121 which has been issued for the first digital device 112.

[00067] In use, the user is then placed in a position where they can then compare the temporary ID 121 appearing on or otherwise associated with second digital device 115 with the temporary ID 121 appearing on or otherwise associated with first digital device 112 during a pre-determined time-frame. In one form, if the two temporary IDs match, then may confirm to first digital device 112 that a match has occurred and trigger by way of choice check-box 126 transmission of an authorisation signal 127 from first digital device 112 to server 111.

[00068] On receipt of the authorisation signal 127 the server then causes the log-in on second digital device 115 to be treated as authenticated thereby allowing the user to access data and services under that log-in user account 113 on server 111.

Alternative Embodiments

[00069] The example embodiment shows the vouching of an authentication to occur between a personal computer and a smartphone with the smartphone being the vouching device. An alternative embodiment could allow any device the user owns or operates to vouch for any device the user wants to add to their account.

[00070] The example embodiment uses a four-digit number to identify the device requesting authentication. An alternative embodiment could use any method to identify the requesting device in such a way so as to ensure that a

user of the vouching device can be reasonably satisfied as to the identity of the requesting device.

[00071] The example embodiment does not specify how the authenticated session between the server and the vouching device is shared with the new device. An alternative embodiment could use a token or a session key. In yet another alternative embodiment actual authentication data from the vouching device could be used in part or in duplicate as a means of allowing a new device to establish its own authentication credentials. For example if a PIN was used to authenticate a vouching device then a system that uses the same PIN on the new device could be used to establish the new authentication credentials.

[00072] The example embodiment shows a new device being authenticated by previously registered device for a secure session. An alternative embodiment could allow the authentication to occur for use in a single session, a limited number of sessions or time period, or indefinitely on a permanent basis.

Date Reçue/Date Received 2023-02-14

CLAIMS

1. In an environment where a first device may communicate with a server subject to authentication of the first device with respect to the server, a method carried out by the server for authenticating a second device comprising:

receiving, from the first device having a first device identity, a first request for establishing an authenticated user's account;

storing the user's account details comprising the first device identity and a username on the server;

receiving, from the second device, a second request to authenticate the second device to use the user's account, wherein the second request comprises the username;

sending, to the second device, a third request to use the primary device to vouch for authentication;

receiving, from the second device, an acceptance of using the first device;

sending, to the second device, a temporary unique identifier;

sending, to the first device, an authentication request comprising the temporary unique identifier;

subject to a confirmation step receiving, from the first device, an authorization to authenticate the second device; and

sending, to the second device, authorization credentials of the first device to access the user's account on the server.

2. The method of claim 1 wherein the confirmation step comprises comparing the temporary unique identifier on the second device and the temporary unique identifier on the first device.

3. The method of claim 1 wherein confirmation is effected if, and only if, the temporary unique identifier on the second device matches with the temporary unique identifier on the first device.

Date Reçue/Date Received 2023-02-14

4. The method of claim 1 wherein the temporary unique identifier is an alpha-numeric sequence.

5. The method of claim 1 wherein authentication may be established for a single session.

6. A non-transitory media encoded with code which, when executed by a processor, performs the method of claim 1.

7. An apparatus for authenticating a second device with respect to a server, comprising:

a. a first device having a first device identity which sends a first request for establishing an authenticated user's account to the server;

b. a memory storing user's account details; the user's account details comprising the first device identity and a username;

c. a second request to authenticate the second device to the user's account being received from the second device; wherein the second request comprises the username;

d. a third request to use the primary device to vouch for authentication being sent to the second device;

e. an acceptance of using the first device received from the second device;

f. a temporary unique identifier being sent to the second device;

g. an authentication request which comprises the temporary unique identifier being sent to the first device;

h. subject to a confirmation step an authorization to authenticate the second device received by the server from the first device; and

i. authorization credentials of the first device to access the user's account being sent to the second device.

Date Reçue/Date Received 2023-02-14

8. The apparatus of claim 7 wherein confirmation is effected if, and only if, the temporary unique identifier on the second device matches with the temporary unique identifier on the first device.

9. The apparatus of claim 7 wherein the temporary unique identifier is an alpha-numeric sequence.

10. The apparatus of claim 7 wherein authentication may be established for a single session.

11. The method of claim 1 wherein protected data is stored with respect to the user account on said server.

12. The method of claim 1 wherein protected data is application data stored with respect to the user account on said server.

13. The method of claim 1 wherein authentication of said first device is effected by entry of a user login identifier and separate authenticating data into said first device.

14. The apparatus of claim 7 wherein said separate authenticating data is a password.

15. The apparatus of claim 7 wherein said separate authenticating data is biometric data.

Date Reçue/Date Received 2023-02-14

Bluetooth Trust System

1. ID 0 and ID 1 identify each other and establish temporary communication.
2. To establish trust between ID 0 and ID 1
   A: ID 0 generates and transmits Temp ID to ID 1
   B: Temp ID displayed on ID 1
   C: If Temp ID on ID 0 equals Temp ID on ID 1 then trust between ID 0 and ID 1.

Prior Art
Figure 1A

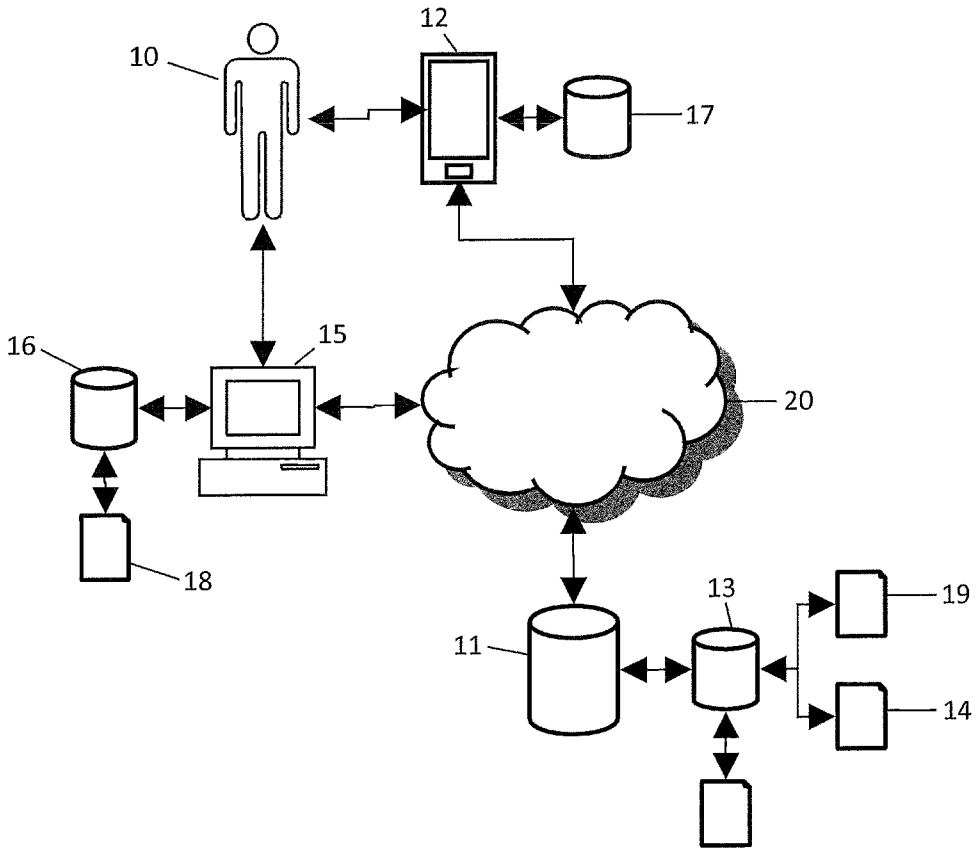


Figure 1B

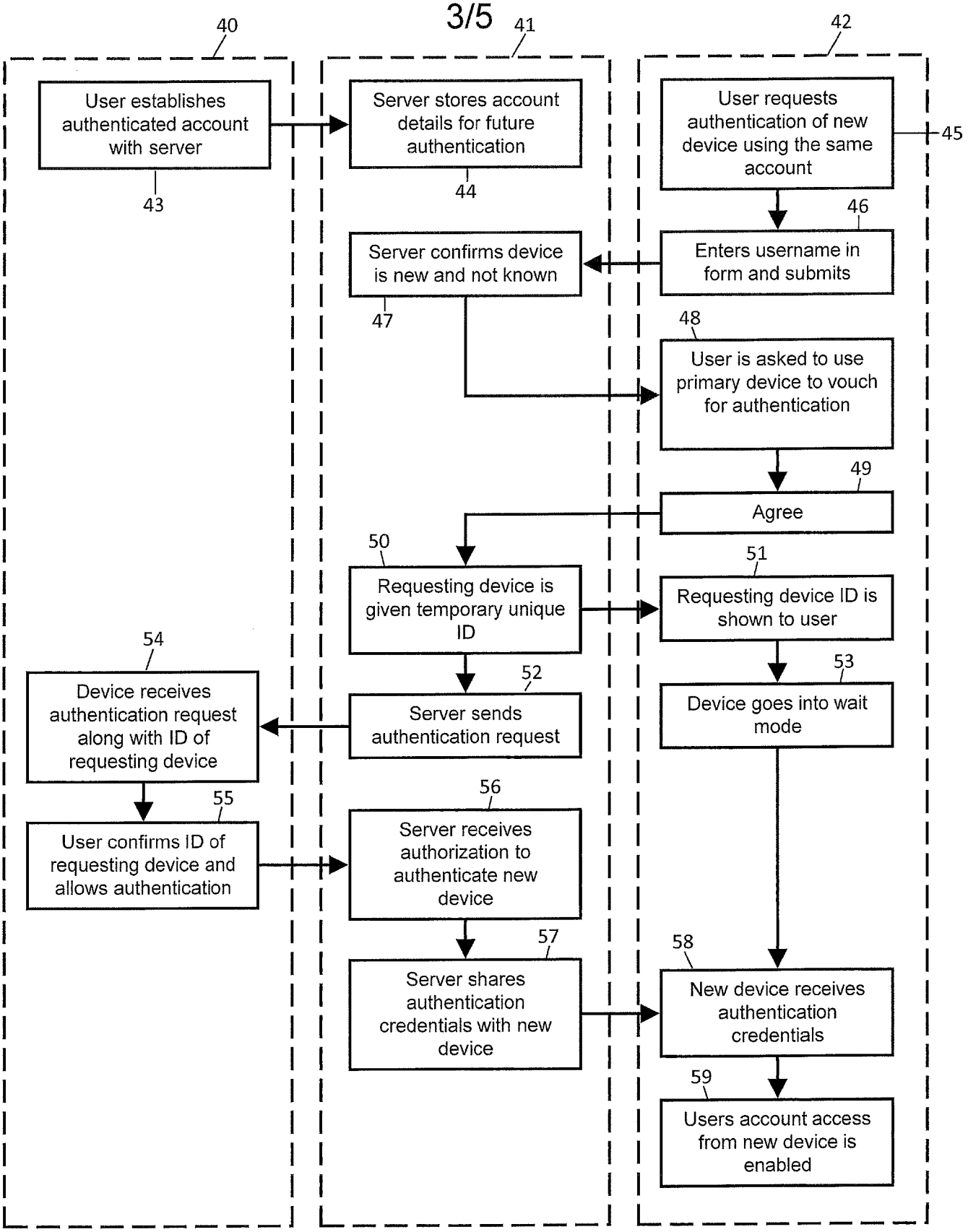
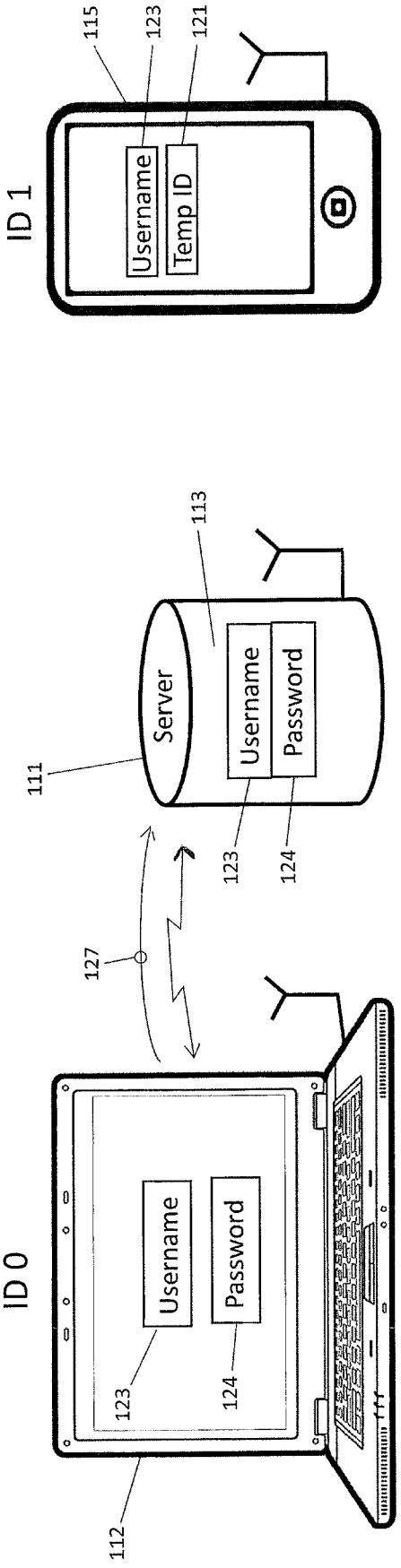

40
41
42
User establishes authenticated account with server
43
Server stores account details for future authentication
44
User requests authentication of new device using the same account
45
46
Enters username in form and submits
Server confirms device is new and not known
47
48
User is asked to use primary device to vouch for authentication
49
Agree
50
Requesting device is given temporary unique ID
51
Requesting device ID is shown to user
53
Device goes into wait mode
52
Server sends authentication request
54
Device receives authentication request along with ID of requesting device
55
User confirms ID of requesting device and allows authentication
56
Server receives authorization to authenticate new device
57
Server shares authentication credentials with new device
58
New device receives authentication credentials
59
Users account access from new device is enabled

Figure 2



1. LOGIN to establish authentication between ID 0 & server for that login

2. To establish authentication between ID 1 and server for that login
   A: Server transmits temp ID to ID 1
   B: Server transmits temp ID to ID 0
   C: If Temp ID on ID 0 equals Temp ID on ID 1 then authenticate between ID 1 and server for that login.

Figure 3

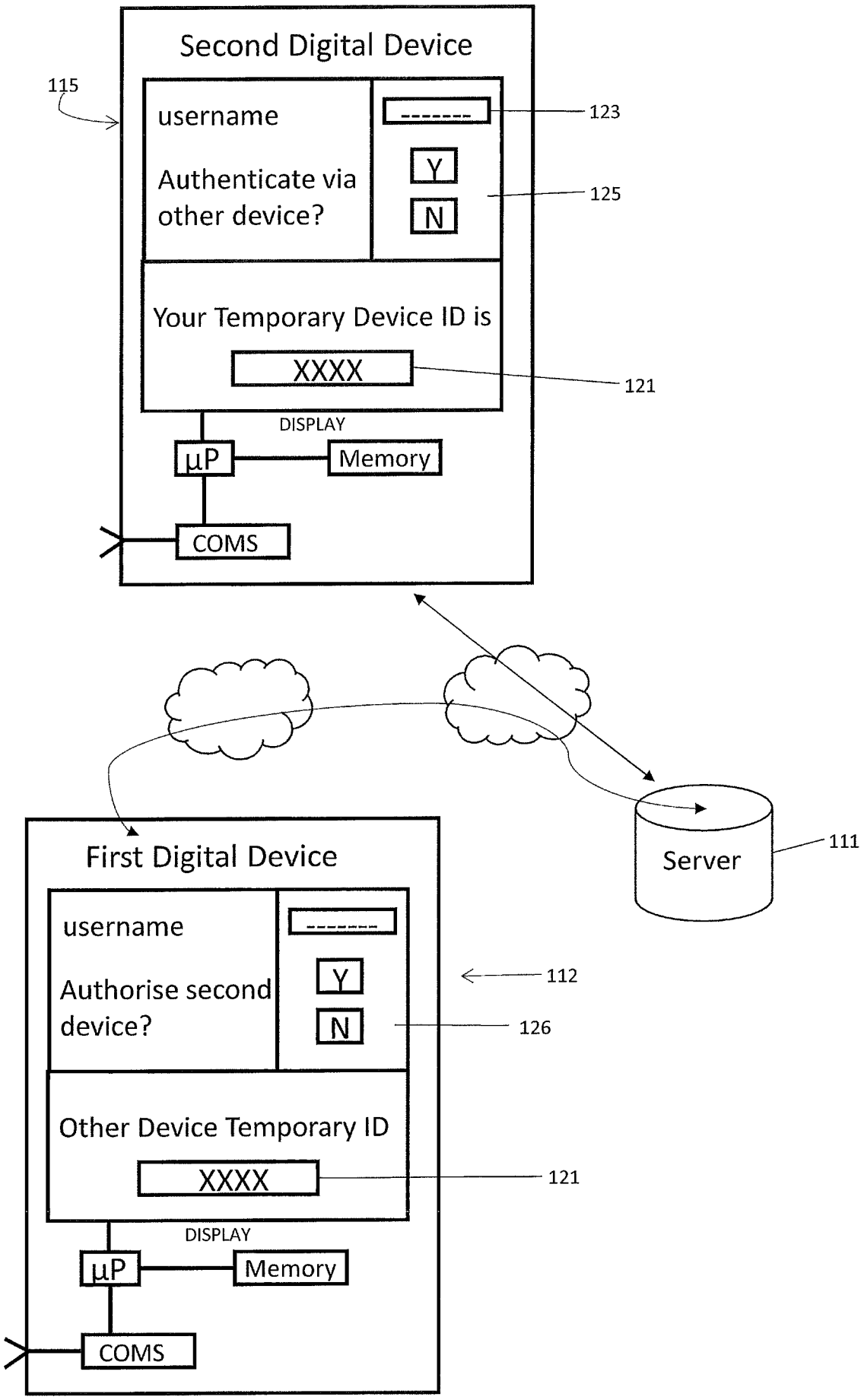
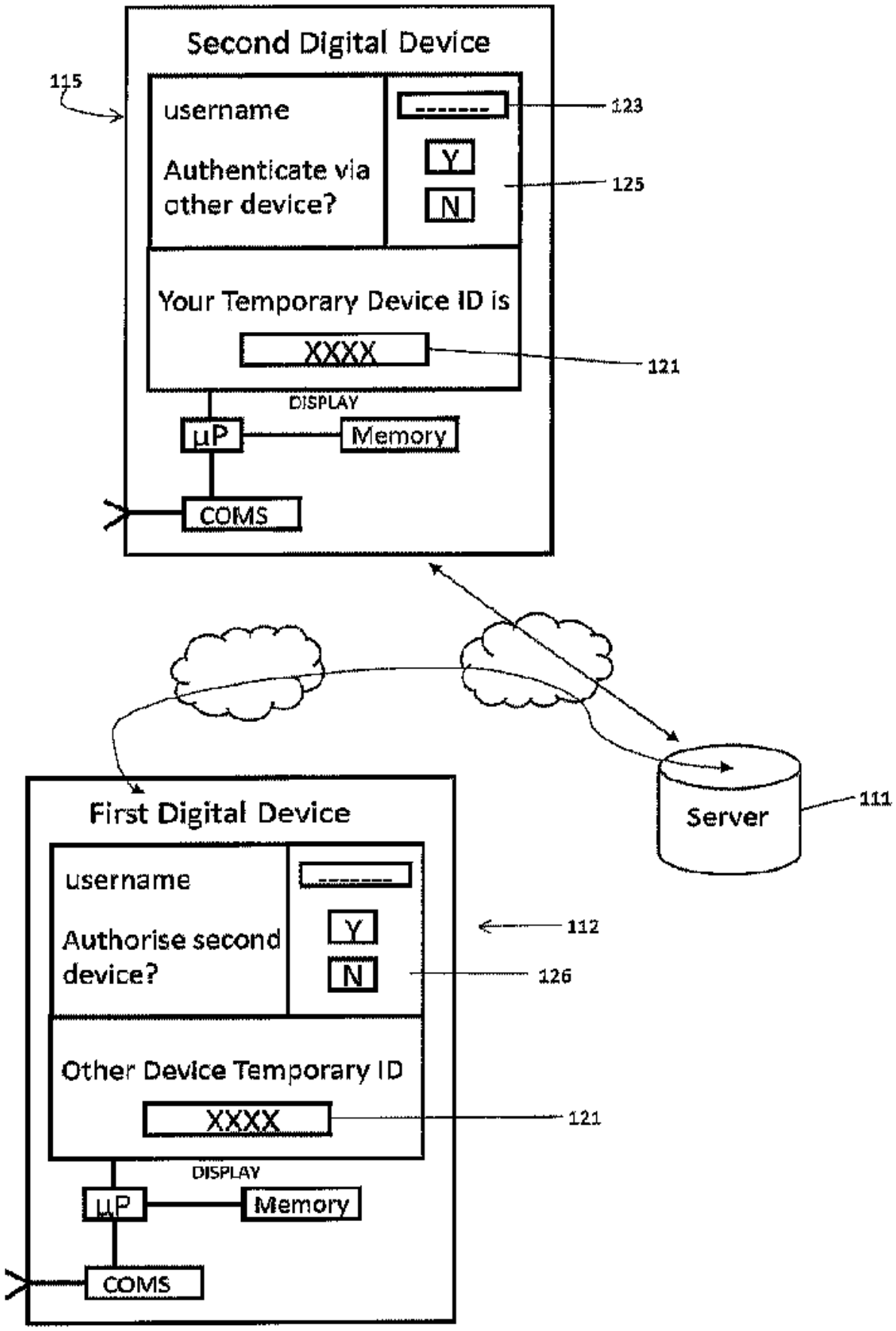

Second Digital Device
115
username
Authenticate via other device?
123
125
Y
N
Your Temporary Device ID is
XXXX
121
DISPLAY
µP
Memory
COMS
Server
111
First Digital Device
username
Authorise second device?
112
Y
N
126
Other Device Temporary ID
XXXX
121
DISPLAY
µP
Memory
COMS

Figure 4


Second Digital Device
115
username
Authenticate via other device?
123
Y
N
125
Your Temporary Device ID is
XXXX
121
DISPLAY
µP
Memory
COMS
Server
111
First Digital Device
username
Authorise second device?
112
Y
N
126
Other Device Temporary ID
XXXX
121
DISPLAY
µP
Memory
COMS